State of Washington
Department of Information Services
Olympia, Washington

Customer Guide
to the Data Center
Disaster Recovery Program

Kenneth Boling, Jr.
Disaster Recovery Program Manager/Coordinator

Contents

I. Introduction

The Department of Information Services (DIS) owns and operates a large computer center that supports data processing services for a number of Washington public agencies. It also operates a large data network which delivers these services to customer agencies in the Olympia area and throughout the state.

DIS is the custodian of these applications and their associated data assets, while the agencies and departments are the owners and ultimate beneficiaries of the automated functions. DIS is responsible for the physical environment and equipment assets. It employs generally accepted systems management practices in its daily operation and in its contingency planning.

A partnership between DIS and the agencies is necessary to protect the applications and information assets within the data center. This partnership must extend to the design, implementation, validation and ongoing maintenance of a recovery capability.

In the event of a disaster that would render either the computer center or the data network unable to provide normal production computing services, DIS has an obligation to restore service in a timely manner. Toward that end, DIS has established a Disaster Recovery Program. This program exists to benefit DIS customer agencies and to encourage joint participation between DIS disaster recovery teams and key disaster recovery personnel within the agencies/departments that use DIS computing services.

Use of this Manual

This Customer Guide describes the program that DIS has set in place and outlines customer agency roles and obligations within this program. It provides steps each customer agency should take to meet their unique recovery requirements. It also suggests actions that agencies may pursue to augment this program. Guidelines for interaction with DIS are also provided.

This Customer Guide contains information available today. Much work is in progress. The guide will be continually updated and quarterly revisions will be distributed to customer disaster recovery contacts in the customer agency organizations as needed.

Program Mission

The mission of the DIS Disaster Recovery Program is:

To develop, demonstrate and sustain a capability to restore the computing environment provided by DIS to customer agencies of the State of Washington **before** the unavailability of these systems causes these customer agencies to experience unacceptable financial losses or organizational disruption and **before** they are rendered unable to meet their obligations to the citizens of Washington State.

The mission of this program is enduring and not expected to change over time.

Program Scope

The DIS Disaster Recovery Program described herein addresses all **production** applications and data supported on the Unisys platform and **production, test and development applications** on the IBM platform, operated by DIS on behalf of its customer agencies. The scope includes production UNISYS computers and IBM computer platforms that are run under the MVS and VM systems. Its scope also includes the data network delivery mechanism provided by DIS to customer agencies.

The following are **excluded** from the scope of this program:

- Test and development platforms on the UNISYS computer
- Facility managed, customer owned equipment, unless a disaster recovery contract has been arranged
- Customer agency: Local Area Networks (LANs), associated file and network services, LAN-attached or stand alone personal computers (PCs),
- Computer Microfilm Output

The scope of the DIS Disaster Recovery Program may be revised over time as a response to new or changing customer requirements. Any modification in scope will be negotiated between DIS and the customer agency.

Program Objectives

Based on the **Business Impact Analysis** conducted by DIS with its Customer Agencies, the current objective of the DIS Disaster Recovery Program is to restore and make accessible to its end users critical and vital operating environments and data within **72 hours** of a disaster declaration.

This 72-hour period was established to be the *outage tolerance* of the overall customer community. If DIS computing services are not provided for more than 72 hours, unacceptable financial losses, organizational disruption and harm to the economy and citizens of the State of Washington may result.

Another objective of the DIS program is to restore application data to currency within 24 hours **before** the disaster. The production readiness of this data must be validated by individual customer agencies. Where more current data or alternate data checkpoints are required for synchronized application system restoration, the customer will be responsible for implementing the necessary data capture and restoration processes.

Objectives of the DIS Disaster Recovery Program are expected to evolve with new technology deployment and a growing dependency on automated functions within its customer agency base.

Conceptual Recovery Time Line

The graphic below depicts the typical progression of steps and activities anticipated within a well orchestrated disaster recovery plan.

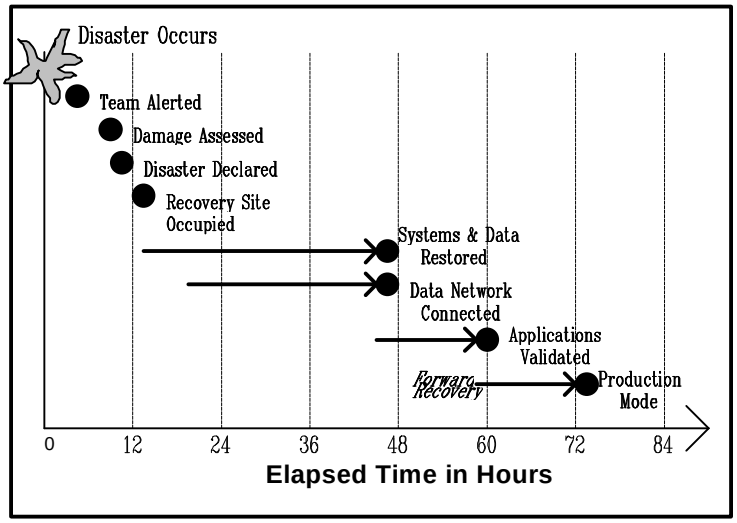

Figure 1

NOTE Customers should not expect any production DIS computing services to be available within the first 72 hours after a disaster declaration. All customer agency business recovery plans should include this as a basic planning assumption.

THIS PAGE IS INTENTIONALLY LEFT BLANK

II. Program History

Background

The Cost of Outage (Business Impact Analysis)

In 1990, DIS executive management began to develop a comprehensive Business Recovery Plan for the department. To establish the requirement, they worked with each client/customer agency to determine their individual cost of outage should DIS services stop functioning. Growth in cost was analyzed as outage time elapsed. The Business Impact Analysis findings were:

- The monthly cost of outage for UNISYS-based customers totals $62 million
- The monthly cost of outage for IBM-based Customers totals $26 million
- The aggregate three-day cost of outage totals $10 million

A loss of more than $10 Million was determined to be unacceptable. As a result, the recovery objective of this program is to ensure restoration of critical systems within 72 hours. There is reason to believe, based on continued deployment of technology and the automation of more basic functions, that the losses realized from a computer outage today would be even more costly.

Hot Site Services

In order to restore applications within 72 hours, DIS subscribes to a Hot Site Service Bureau for both UNISYS and IBM services. A **hot site** is a location containing computers and necessary peripheral equipment that may be occupied by a subscriber immediately after a disaster declaration to restore its own systems, applications and data.

A hot site is a shared facility with a number of subscribers from different geographic locations, each of which share in the cost of maintaining the fully operational center. Each subscriber may occupy the hot site for up to six weeks after a disaster. These facilities are also available for subscribers to exercise their recovery plan in test mode.

Hot site recovery is appropriate for a computer operation that has a 24+ hour outage tolerance. Data centers requiring faster service restoration must invest in redundant (spare) equipment that is immediately available to satisfy this need. Conversely, facilities that can afford to wait several weeks before restoring service need not engage a hot site for they will have time to order and install new equipment.

From a competitive bid process, the following hot site providers were selected:

- UNISYS: SunGard Recovery Services, Warminster, PA
- IBM: IBM Business Recovery Services, Gaithersburg, MD

These two providers offer sufficient computer power, disk space, tape drives, and related equipment to satisfy DIS recovery requirements.

Cold Site Services

Both SunGard and IBM Business Recovery Services augment their hot site service offering with a **cold site** feature. These are facilities designed to receive computer equipment. All power, water, air conditioning, raised floor and other items requiring a long lead time to acquire, install and make ready to house a computer center are in place.

Should DIS be unable to return to its home computing center within six weeks of the disaster, it would make arrangements to occupy these cold sites. Computers, peripheral equipment and related services would be ordered (purchased, leased or rented) and made ready to assume the DIS processing workload. Cold sites may be used for an additional six months, allowing DIS sufficient time to repair or rebuild at the home site.

The hot sites and cold sites are half of the recovery equation. DIS must also provide access to the restored data center operations to its customer agencies and their end-user community.

Data Network Backup Design

The other half of the recovery requirement is to devise a mechanism to provide end-user access to the two hot sites. End-user locations on the data network need to connect to their restored applications and data after the disaster. This need has been addressed by a powerful data network switching capability.

There are two major types of connections within the DIS network:

- Local Data Services that connect via the Telephone Company (non-DTS) to DIS Front-End processors.
- Remote circuits within DIS' Digital Transport System (DTS) that connect to a DTS node site and are then transported over the high speed backbone from a number of locations throughout the state to a Front-End processor in the DIS computer center

Separate backup designs were necessary for each.

Local/Digital Services

The Data Network Services Disaster Recovery Strategy addresses implementing the recovery of Telecommunications Services Division (TSD), Local Data Services (LDS) and Digital Transport Services (DTS) that may be affected by a disaster in Office Building Two (OB-02). LDS are those **non-DTS** network circuit connections direct from the DIS OB-02 Data Center to customers in the Olympia and surround areas, such as Shelton, Aberdeen, South Bend, Centralia, etc. DTS are distinct from LDS, in that DTS serves geographically more distant customers using high bandwidth transport technology from a concentration point in Seattle, Washington.

In the event of a disaster affecting OB-02, LDS recovery is accomplished through the TSD Lacey Network Center (LNC). **Approximately 50 percent of the existing local circuits, both shared and dedicated, have been re-homed to this second Front-End location**. The recovery procedures will establish cross-country communications lines from the LNC to the platforms at each hot site using AT&T Accunet Reserve circuits. The lines directly terminating at OB-02 will not be recovered.

DTS recovery is accomplished by routing the DTS circuits (from Seattle, Yakima, Vancouver and Spokane) through AT&T Accunet Reserve circuits to the mainframe recovery hot sites. **100 percent of the DTS traffic will be recovered.**

Network Node Sites

Network Node Site Disaster Recovery Team will, in the event of the loss of a Node Site, provide emergency interim Network Services until full restoration of the Node Site can be accomplished. The architecture of the network protects other Node locations from isolation in the event one of the Node Sites is lost. The loss of a single Node Site will affect only the customers served directly from that node. Service to the remainder of the network will be undisturbed. Subsequent to a disaster, the Team may use one or a combination of alternative strategies to establish emergency interim network services, depending on the nature and location of the disaster. The alternatives include:

Under one strategy the NNSDR Team would request the Local Exchange Carrier (LEC) to re-connect the circuit(s) which were between the local Central Office (CO) and the disabled Node Site to the closest operational Node Site (e.g., Spokane is disabled; run circuit to Yakima). LAD circuits cannot be recovered in this manner. Only circuits with matching modems in the "backup" node will be recoverable. Clients at both nodes will be required to work on a restricted basis, which would most likely include balancing hours of use with some off-shift scheduling in order to accommodate the additional throughput.

An alternative (or additive) strategy would be to request the LEC to provide a DS1 from the local CO to the nearest operational site, and to multiplex the local DSO circuits across it. The traffic could then ride the existing DTS DS3 network to Olympia. A DS1 Channel Bank would be installed in Olympia to de-Mux these circuits. A viable but costly variation of this alternative would be to run IXC circuits from the local CO (at the disabled Node Site) to the Olympia CO, and LEC tail circuits to OB-02.

Another effective but very costly alternative would be for DIS/TSD to invest in a "Mobile Node Site" fully configured to replace all equipment at a node. In the event that a Node Site is disabled, Mobile Node would be moved to a convenient location adjacent to the CO, and the LEC would be requested to re-connect circuit(s) it to the circuits from the disabled. The DS3 vendor would also re-connect its service at the Mobile Node.

Finally, full recovery for the disabled Node Site will focus on relocating to an alternate site (if required), and the rapid repair, procurement and deployment of equipment, and re-termination of circuits at that location.

Conceptual Diagram

Below is a conceptual diagram of this backup capability.

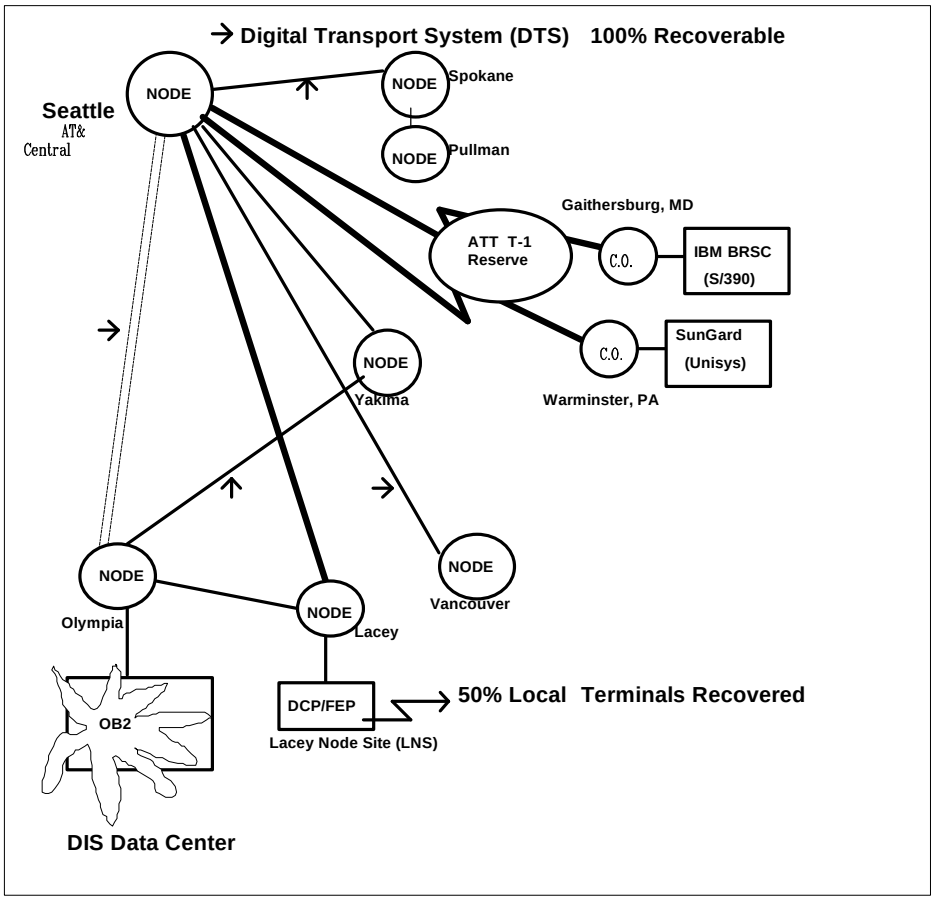

Figure 2

Other Network Services

Network Support Center (Helpdesk)

The Network Support Center (commonly known as the helpdesk) provides telephone "hot-line" diagnostic and consultative assistance to customers of DIS information services 24 hours/day, 7 days a week. In the event of a disaster affecting OB-02, the Network Support Center would most likely be displaced.

INITIAL STRATEGY

During the initial 72 hours following the declaration of the disaster, the Network Support Center (NSC) Helpdesk will utilize whatever space is available, which could include the NSC evacuation site in the Adams Building and any vacant DIS offices with working phones. The NSC Centrex phone lines will be call-forwarded to these phones and the helpdesk will be able to provide management approved status notification to customers about the disaster, the recovery efforts, as well as take customer query calls. Copies of all required documentation will be stored in the Adams Building evacuation site for use during an OB-02 disaster or evacuation.

Short-Term Strategy

During the initial 72 hours, DIS staff with vendor support, will be implementing a short-term helpdesk in the 2nd floor conference room of the 512 Building. This will consist of desks, chairs, installing S390 and UNISYS terminals, and a bank of phones. Upon completion of this installation, the NSC will call-forward the original helpdesk phone numbers to the new phone bank and the NSC staff will relocate and begin providing current helpdesk support.

Resources required would include S390 terminal access for support of the S390 mainframe and network support (this constitutes about 56% of NSC problem calls); either UNISYS terminals or a crossdomain connection between UNISYS and S390 to access UNISYS via the S390 network connections, and; X.25 terminal access to provide X.25 customer support. SCAN and PBX support does not require any special equipment at the helpdesk.

Long-Term Strategy

Complete long-term recovery of the helpdesk function in a permanent location would include replacement of the ACD or equivalent for call distribution, CNS system replacement, individual workstations and terminals and access for all services the NSC currently supports.

Dial Access Service

"Dial-Access" is a DIS dial-up service that is supported by value-added network provider, MCI Communications (MCI). It supports dial-up connectivity from customer workstations to DIS S/390 and UNISYS 2200 computing environments, or private customer hosts. Dial-Access currently supports over 1,100 dial-up users representing in excess of 100 agencies/private entities. MCI has installed a local node in the OB2 DIS computer facility that supports Olympia dial-up traffic.

The Dial-Access Service has host interface circuits for the SYSTEM/390 and the UNISYS Data Centers that connect to the Lacey Node Site. Should the OB2 facility suffer a disaster, the Dial-Access Service will have functional host interfaces to the DIS Disaster Recovery Hot Sites via the Lacey Node Site. Dial in access will be provided via MCI Data Services access number at their PUBLIC Olympia node for 2400 kbps. This is NOT the same access number that DIS Dial-Access Service customers currently use. The current Olympia number for 2400 kbps is a private access number accessible only by DIS Dial-Access customers. Dial in access for 9600 kbps will be provide via alternate MCI Data Services access numbers throughout the state. These numbers are currently available to all DIS Dial-Access Services customers. There are over 1,000 MCI access numbers available worldwide. Information on the alternative routing would be made available directly to the customers, and through the DIS Dial-Access Support Center.

X.25 Network Services

The X.25 Network Service provides a statewide X.25 network that facilitates access and connectivity to mainframe, mini-computer, and LAN platforms. X.25 network remote switches are located in the Seattle, Vancouver, Spokane and Yakima node sites.

DOS/VFS: In the event that X.25 equipment located at OB2 becomes unusable, the Seattle X.25 will become the temporary management hub. An Auxiliary Service Processor (ASP) installed in the Seattle X.25 switch will allow call setups to continue. DR backup 56KB links between Seattle to Spokane, Yakima, and Vancouver will be enabled using the DIS Advanced Transport Service (ATS).

NOTE: DOL/VFS has no DR plan in place to provide an alternate site for the four (4) production HP3000 mini-computers located in OB2. Thus, if OB-2 becomes unavailable, the X.25 network will be available, but there is no processing hot site to support the DOL production work.

WUTC: UTC has three (3) sites: Olympia, Kent and Spokane. Loss of the OB-2 facility would require the Olympia office to dial into the Seattle X.25. DIS will supply the 9600 bps modems and any other X.25 hardware to make this dial connection

Disaster Recovery for the DIS Router Network AT OB2

STRATEGY: The DIS Router Network service provides a router-based backbone at the DIS Data Center, located in Office Building Two (OB2) with backup facilities at the

DIS Lacey Node Site (LNS). The router backbone facilitates access and connectivity to DIS and customer host systems or local area networks. Router network hubs are located at the OB2-East, OB2 West, and Lacey node sites.

In the event that Router network equipment located at OB2 becomes inoperable, the LNS will become the main router network hub. Router network traffic will be routed to available DIS and customer host systems or local area networks that are connected to the LNS router.

In a disaster recovery situation that effects the entire DIS OB2 Data Center, TCP/IP traffic will be delivered to the System 390 and Unisys disaster recovery hot sites via the IBM NCP and Unisys DCP Front-End processors locate at the LNS.

Notes: Customers that want backup for their router-based networks and are connected to the DIS Router Network hub at OB2, must install secondary router connections from their router network location to the DIS backup network router hub located at the LNS.

Currently, this plan does not address backup for access to the INTERNET.

Local Telephone Service

The Telecommunication Services Division Local Telephone Services (LTS) organization provides local telephone service to governmental entities on a statewide basis. This service is provided either through a contractual agreement that DIS has negotiated with a particular local telephone company, or through a DIS-owned Private Branch Exchange (PBX).

In the event of a disaster which destroys a serving vehicle, or otherwise disrupts local telephone service, the LTS Disaster Recovery Team is to provide dial tone and access to the Public Switched Network (PSN) for its affected customers. The LTS Disaster Recovery Team will coordinate initial, interim, and full service restoration. The specific strategy is unique to a given disaster scenario. Key tasks for all recovery strategies will include:

1. Assessing requirements and establish priorities with customers.
2. Placing necessary servicerequests with vendors and providing vendor coordination.
3. Providing status and cost information to the Telecommunications Disaster Recovery Group, and status information to customers.
4. Monitoring service installation and delivery.

Long Distance Telephone Service

All TSD long distance services are discretionary services that take advantage of government's aggregate purchasing power. They are offered to state and local government as an alternative for reducing costs for the same services offered by the public switched network (PSN). The loss of any TSD long distance service does not preclude any customer from immediate alternative long distance service from the public switched network.

Scan

The Long Distance Telephone Service (LDS) Disaster Recovery Plan assumes the loss of a single SCAN switching location causing disruption to the services of state and local government clients served by it. The initial recovery strategy is based on the immediate use of the alternative (dial 9) toll long distance telephone services for all clients. This would be followed by an interim recovery period during which supplemental high capacity LDS would be provided by the current DIS contracted carrier to selected clients. The recovery team would subsequently concentrate on restoring the damaged resources and facilities.

Scan Plus

The Long Distance Telephone Disaster Recovery Plan assumes the loss of an isolated geographical area or major outage of the SPRINT public network[1]. The full recovery strategy is based on the immediate use of alternative toll long distance providers for all clients (billed to hotel, pay phone, collect to destination, etc.), until SPRINT's network problem is resolved.

TSD Toll

This toll service is only available to, and therefore could affect, DIS local telephone service customers. The Long Distance Telephone Disaster Recovery Plan assumes the DIS Primary Inter-exchange Carrier (PIC), currently MCI, suffers a major network outage. The full recovery strategy is based on the immediate use of alternative PIC choices by using public switched network dial access codes (10-XXX). There is no alternative if the local exchange company intra-lata long distance network becomes impaired.

Washington Interactive Television (WIT) Services

The Department of Information Services Washington Interactive Television (WIT) is the statewide video telecommunications system offering complete services including an Olympia area broadcast-quality television studio, post-production services, satellite services, cable channel coordination, and two-way interactive Video conferencing at 13 sites throughout the state to make communication faster, easier, less expensive, and more effective for the government, education, and citizens.

In the event of a disaster, WIT is responsible for coordinating the restoration of WIT services. These services are designated as non-essential, and thus are not critical for immediate recovery

[1] Sprint and MCI employ reasonable failure protective strategies including network redundancies, UPS, generator backup at key equipment sites, and emergency response teams.

State Telephone Operators

Directory Assistance

The initial recovery strategy is to copy the "FOX PRO" data base to the Banyan network (and diskette) as a backup and in the event of an emergency acquire 10 PC's, reload the FoxPro version of the directory onto the data base, load the lookup programs, and by using "plain vanilla telephones", have US West redirect the calls to the new locations, and the operator's will provide information to callers. The long term strategy will be to re-establish the "Automated Attendant system."

Conference Call Service

The recovery strategy is to provide a voice message, and let agency telecommunication coordinators know that a third party vendor (for example, AT&T) will be providing Conference Call Service until DIS would be able to reestablish the lost service.

Voice Processing Service (SIMON)

Voice Processing Service is an outsourced service provided by U.S. Intelco Networks and U S WEST Communications.

The State Interagency Messaging Network (SIMON) provides voice processing service to more than ninety customers via twelve nodes (sites) throughout the State. As of April, 1993, there were more than 11,000 mailboxes system wide providing voice mail, telephone answering, call routing, bulletin, and other special application mailboxes.

If any one of the voice processing units goes completely out of service, the vendor will provide a hot standby unit from one of two locations. The vendor's disaster recovery team will install the hardware and software within two business days of notification.

Should the system drives of the unit be damaged, all mailbox configurations and messages would be lost. In this situation, the ordering database would be used to rebuild the mailbox configuration database, and could be accomplished within one business day. If the system drives are not damaged, no messages or mailbox configurations would be lost.

Cellular Phone Service

Cellular telephone service is provided to DIS customers through master contracts with US West Cellular and Cellular One. It is important to note that during a disaster, cellular to landline phone transmissions may be interrupted due to landline outages. Both vendors have disaster prevention and recovery strategies to minimize outages for cellular to cellular phone transmissions, however. The disaster prevention and recovery strategies of these vendors are as follows:

US West Cellular

The system has two main switch sites (one in Tacoma and one in Bellevue), which have fiber optic redundancy. Via FLASH reporting, US WEST Cellular Maintenance Personnel instantaneously receive messages regarding outages. If the Seattle site goes down, the other system could handle the calls through alternate pathway. All cell sites have battery (UPS) and generator back-up capability. The emergency generator is on-line within 30 seconds and has a 2000 gallon fuel capacity. US WEST also has two disaster recover rooms: one at the Network Operations Center (NOC) in Bellevue and one Phoenix, AZ for disaster recovery management.

All cell sites are wired for portable generators. US WEST has 45 fixed generators and 15 portable generators strategically placed for deployment if necessary. All cell sites are wired for portable generators. If cell sites fail, emergency teams would isolate and repair the problems. Additionally, US WEST has three transportable cells sites to deploy in the event of an emergency.

Cellular One

The three major subsystems of the Cellular One network in Washington state are the Mobile Telephone Switching Office (MTSO), the interconnect facilities, and the cell sites. All are engineered for protection, efficiency and redundancy. The system configuration has power backup redundancy features through the use of multiple transmit and receive antennas. Spare transmission lines have also been installed at each site for backup purposes. All three of the Cellular One switch sites (MTSOs) have battery back-up (UPS) and diesel generators. In the event of failure, traffic could be switched from the Seattle site to sites in Spokane or Portland.

All cell sites have 4 to 8 hour battery back-up and 25 percent of these sites also have generators. For those sites without generators, when a power outages persist beyond the 8 hours, Cellular One's practice has been to have emergency personnel rapidly move generators to the location. Additionally, Cellular One has three temporary transportable cell sites to deploy in emergency situations. System performance is monitored at the national Network Operations Support Center 24 hours a day, seven days per week and system technicians have been trained to respond to a variety of outages.

Paging Service

Paging service is provided to DIS customers through a master contract with Cook Paging. The vendor's disaster prevention and recovery strategy is as follows:

In the event of a natural disaster, all technical staff will return to the Cook Paging Seattle office. System diagnostic testing will be performed to determine if any outages are present and technical staff will be dispatched for immediate problem repair. Per the Cook Paging emergency call list, major customer will be notified of down-time, expected duration and will be called when the system in on-line again. As an emergency communications service provider, Cook Paging, as well as other paging carriers, receive first priority for phone line repair.

Cook Paging has a 50,000 pager unit capacity with approximately 28,000 units on the system. Their main computer (which relays messages to the main link transmitter) is located in Seattle and has an eight to twelve-hour UPS battery back-up. In the event the battery system fails, or the outage exceeds the eight to twelve hours, Cook has a propane (LPG) driven generator to provide power supply. LPG was selected due to propane availability and transportability during disasters.

Control of the paging system main computer in Seattle to main link transmitter is operated by radio frequency eliminating the need to depend on phone lines for control transmission. This enables operation of the paging system even if phone lines are damaged between Seattle and the main link transmitter. Cook has also negotiated an agreement with KUBE FM radio to utilize their generator for the Cook main link transmitter. This generator is rated for 12 days. Fifty percent of the mini-transmitters, which relay messages from the main transmitter, have either battery or generator back-up power. If any of the mini-transmitters fail, and alarm sounds at the main computer and system engineers will repair/replace the mini-transmitters.

Washington Information Network (WIN)

WIN is a “proof of concept” pilot demonstration project. The purpose of the project is to test the viability and feasibility of providing direct service delivery of government information and services via ten information kiosks. This pilot project will run from June 1994 through June 1995. If WIN becomes production following this pilot period, DIS will expand the recovery strategy.

The WIN system will use disaster recovery procedures that are provided by the DIS Computer Services Division and the DIS Telecommunications Services Division. All WIN software application programs will be maintained off site at North Communications, located in Santa Monica, CA. North Communications will maintain dial-up access to the WIN host server for the purpose of providing planned and emergency maintenance support for the WIN application.

Disaster recovery at the kiosk sites will be handled on a case-by-case basis during the operational period of the WIN pilot demonstration project.

External Business Services

Policy and Regulation Services

Legislative Assessment, Vendor Protest Reviews, Information Services Board Book Preparation - The Policy and Regulation Division (PRD) will support divisional work from employee homes using existing home computers until the DIS facilities team can provide an alternate site location for the PRD staff. Information technology required by the PRD staff includes Word, EXCEL, OfficeVision, and MSMail.

PRD staff will access available LAN dial-up ports for data access and printing support. Protest reviews, legislative assessments, and ISB book work-in-progress, will be restored from the LAN backup file to another DIS server. In the event that LAN backup files are not available, PRD will

request copies of required documentation from vendor(s) and agency(ies). Voice mail messaging will be used to notify incoming callers of the alternate phone number(s) that may be used to reach PRD staff.

Other PRD Services

Other services provided by PRD, including acquisition reviews, policy formulation, proviso project support, and strategic planning will be supported throughout the recovery effort.

Agency Systems and Programming Support

The Agency Systems and Programming (ASP) section within DIS develops and maintains applications for contracted customer agencies with limited or no information technology staff of their own. In the event of a disaster, the support team will provide the following support for ASP maintained systems:

Disaster at the Mainframe Site

In the event of a disaster at the mainframe site, the ASP team will insure that backup files and documentation are available, ASP will obtain copies from agencies and/or vendors. ASP staff will provide processing priorities for customer agency applications and assist in distribution of output. Data access will be through existing LAN dial up ports.

Disaster at the Primary Site

In the event of a disaster at the primary site, ASP will move necessary staff to the alternate DIS site designated by the DIS Facilities Recovery Team, assess the status of jobs in progress and work with external agency customers to insure their jobs run correctly.

Systems Recovery at the Alternate Site

ASP will assess system and DASD recovery status for ASP maintained external customer systems at the alternate site, and provide any support that is needed for recovery, maintenance and continued operation.

Equipment Maintenance Services

The Equipment Maintenance Service provides maintenance solutions for computer workstation, data communications equipment, and electronic peripherals on a state-wide basis. There are technicians located on-site in Olympia, Seattle, Tacoma, Spokane, Wenatchee, and Yakima, as well as a maintenance depot in Olympia providing "over-the-counter" repair service.

Any disaster destroying or disabling the Olympia maintenance depot could severely curtail DIS' ability to continue the service. An alternate facility and replacement equipment could be assembled within two to four weeks,

however some of the parts inventory which includes rare and unique items, would be difficult to replace. Plans are being implemented to distribute unique inventory items to multiple statewide locations; providing better response times and alternate inventory facilities. By utilizing the alternate inventory facilities and the shifting of other resources and personnel, the service will be able to provide the contracted maintenance customers' agency critical applications with immediate/continued support.

Disaster losses outside Olympia would be restricted to the vehicle, some test equipment, and a small parts inventory. Recovery strategy would involve shifting of resources and rescheduling. Clients would not suffer a serious loss of service.

Equipment Brokering and Leasing Services

The DIS Brokering and Leasing section provides a cost-effective, centralized acquisition function for information technology equipment and software to more than 120 state agencies and 150 local government organizations. The state's information technology community realizes significant savings from the labor-saving support, technology recommendations, and collective purchasing power provided by this unit. Many agencies, including DIS, are depending on Brokering and Leasing's ability to rapidly deploy its resources to locate, acquire, and install replacement equipment needed in the event of a disaster.

In the event of the loss of the Equipment Brokering and Leasing facility, the Equipment Brokering and Leasing Services Support Team (EBBSS) will provide emergency interim services until full restoration of the facility can be accomplished. The team will concentrate on damage assessment and notification procedures, and attempt to restore or replace equipment inventory, customer purchasing records, and customer owned equipment.

Internal Services

DIS Facilities Recovery

The recovery strategy for DIS facilities is to oversee the damage assessment and recovery of a physical structure and equipment housed within that structure. Assesses damage to the general office areas. Manages the securing and moving to a temporary relocation facility and provides support to project management in repair and replacement of the facility and its contents. They will configure conference rooms and extra space in existing DIS facilities to enable short-term use of these areas for DIS staff to continue providing service. The team will acquire PCs, basic telephones, desks, etc. at the time of the disaster to meet the requirements. The LAN/Workstation Support Team works with the Facilities Recovery Team to accomplish this recovery task.

Lan/Workstation Service

The LAN recovery plan focuses on recovering from loss of one major facility serving DIS personnel. In the event of such a disaster, one or more

of the multiple LAN back-up servers would be moved from its safe-storage site, and added to the DIS Wide Area Network (WAN). The plan assumes that "public terminals" would be set up for shared use by members of the displaced staff in DIS conference rooms and training facilities that have available wiring. As an alternative, displaced workers would share work space with other DIS employees until equipment for additional ports could be acquired and installed.

Disaster Management Support

Administration Support

The Administration Support Team provides administrative support for disaster team activities; assists in the preparation of insurance claims; types team documentation and collects/coordinates team reports and information; and assists with disaster notification of Recovery Teams. The Administration Support Team will make use of the Control Center or other DIS facilities to provide these services.

Logistic Support

The Logistics Support Team provides procurement of goods and services, transportation, mail processing, warehousing and furniture installation and repair. The Logistics Support Team works with the Disaster Management Team to recover business processing if a disaster occurs at the business site and provides assistance to other units if disaster occurs at other DIS sites. The recovery strategy is to make use of other available DIS facilities for basic technology requirements so that service can continue. The DIS Facilities Recovery and the LAN/Workstation Support Teams will assist in this strategy.

Travel Support

The Travel Support Team works with the Disaster Management Team to assist the disaster recovery teams in making arrangements for travel to alternate sites for disaster recovery. This assistance includes hotel accommodations, airline reservations and rental cars.

Human Resources Support

The Human Resources Support Team works with the Disaster Management Team to coordinate human resource activities and resolve human resource issues; determine status of personnel adversely effected by the disaster; and coordinates replacement personnel requirements. This team also recovers the human resource services if a disaster occurs in the building housing this function. The recovery strategy is to make use of other available DIS facilities for basic technology requirements so that service can continue. The DIS Facilities Recovery and the LAN/Workstation Support Teams will assist in this strategy.

Communications Services Support

The Communications Services Support Team works with the Disaster Management Team to gather accurate disaster information and promptly inform management, customers, employees and the general public using appropriate communication channels. The recovery strategy is to make use of other available DIS facilities for basic technology requirements so that service can continue. The DIS Facilities Recovery and the LAN/Workstation Support Teams will assist in this strategy.

Internal Information Technology Recovery

In the event of a disaster at the mainframe site, the Internal Information Technology Recovery Team will assess the status of internal applications that were not completed correctly, assess system and DASD recovery status at the alternate site, oversee the running of priority internal applications at the alternate site and review with the internal customers the output generated from the alternate site.

In the event of a disaster at the primary business site, the Internal Information Technology Recovery Team will move necessary staff to the alternate DIS site designated by the Facilities Recovery Team, assess the status of jobs in progress and work with the internal customers to insure internal applications run correctly.

Financial Support

The Financial Support Team provides emergency financial support for those involved in disaster recovery for DIS. The team will acquire funds from the Treasurer's office and oversee emergency financial transactions during a disaster. The team will also recover the accounting and payroll functions of DIS if a disaster occurs in the building that houses these functions. The recovery strategy is to make use of other available DIS facilities for basic technology requirements so that service can continue. The DIS Facilities Recovery and the LAN/Workstation Support Teams will assist in this strategy.

Accomplishments to Date

Computer System Restoration Process

After selecting its hot site providers, DIS immediately launched an implementation project. Separate processing teams were formed to address the technical challenges of the UNISYS and IBM platforms, as well as the common logistic issues of data capture, off-site storage and transfer to the hot sites. Early exercises were conducted as "proof of concept" for the hot site approach. Results were positive.

The following demonstrations have been successfully concluded:

System	Date	Objectives	%
IBM	11/91	Proof of Concept • Restore 2 MVS systems • Use data from center	100%
	1/92	Full System Restoration • Use off-site weekly data • Restore all 4 MVS systems • Activate all production CICS • Validate dialed remote access • Validate operation control from Seattle remote customer suite	100%
	7/92	Data Recovery Demonstration • Use off-site daily data • Restore all 4 MVS systems • Restore all production data to "day before disaster" • Restore all CICS and ADABAS • Conduct functional tests from Seattle remote customer suite	95%
	1/93	Above, plus restore of VM System	95%
	10/93	Above, plus test Vanilla System	100%
	4/94	Above, plus testing of Lacey Node	100%
	10/94	Above, plus Lacey Node,Dial Access, Cust	100%
UNISYS	2/92	Proof of concept: • Restore from Center data • Activate System	100%
	8/92	Customer Agency Pilot: • Restore from off-site data • Activate system • Validate dialed access via Front-End • Restore and exercise D.O.L production application	90%
	1/93	Above, plus testing of DMS 11	100%
	10/93	Above, plus PlanIt, and User testing	100%
	4/94	Above, plus testing Lacey Node	100%
	10/94	Above, plus Lacey Node, Customers	100%
Network	1/93	Proof of concept for Remote Digital Transport Service (DTS) to both IBM and UNISYS recovery centers	100%
	10/93	Connect for user testing	100%

	4/94	Proof of Concept for Lacey Node	98%

System	Date	Objectives	%
	4/94	Proof of Concept for Lacey Node	98%
	10/94	Lacey Node, Router,Dial Access	100%
	5/95	General testing	100%
	10/95	General testing/Network/Dial Access	100%

Backup Data Network Design

Backup capability for remote circuits was in place by January 1, 1993. A "proof of concept" demonstration, involving the switching of these circuits to the two east coast hot sites, was conducted in January.

Backup capability for local circuits will be available in November, 1993. This will involve a phased migration of approximately 50% of these circuits to the second Front-End processor. A "proof of concept" for this service, involving the switching of the second Front-End processors in Warminster, PA and Gaithersburg, MD and the ability to inter-connect the Unisys and IBM processors (at Sungard and the IBM Business Recovery Services Center will be conducted in January, 1994.

Disaster Prevention Measures

The only thing better than being able to recovery from a disaster is avoiding one in the first place. DIS has taken a number of steps to limit the likelihood of a computing outage in the data center:

- Access controls, alarms and scanning equipment
- Backup generators
- Sprinklers and halon fire suppression systems
- Physical systems monitoring equipment
- Alternate/spare components for critical equipment
- Operational recovery procedures and practices

Command Center

When disaster strikes, the data center may not be accessible. To ensure that critical decisions can be made and recovery procedures coordinated in a timely manner, the DIS Disaster Recovery Program has identified a series of alternate locations where the executive and recovery management teams can meet and confer with damage assessment personnel.

These diverse locations are designed to provide maximum redundancy and alternatives to meet a variety of unpredictable circumstances. The command centers include:

- A local DIS Olympia location
- An alternate DIS location
- A IBM location in Olympia
- Tyee hotel

The person who, as circumstance dictates and according to pre-planned notification trees, inaugurates the disaster alert process will also select the command center location that is appropriate to the emergency situation. He or she will direct all other disaster recovery personnel who have roles to fulfill during the initial assessment phase to the named command center.

THIS PAGE IS INTENTIONALLY LEFT BLANK

III. Program Organization

Executive Team

The executive team of DIS' disaster recovery team is staffed by executive management of the department. This team has the responsibility to provide executive-level decisions in the period following a disaster, and the authority to declare a disaster and mobilize teams to recover at the hot sites. This decision will be made after input from the damage assessment process.

The executive team will make policy decisions, oversee customer and external communications, and serve as the official source of information during the recovery process.

Disaster Management Team

It is the role of the disaster management team to provide the overall direction of recovery operations. Activities will be coordinated under the direction of the executive team.

The disaster management team will establish the emergency command center where damage assessment and recovery operations will be directed. It will analyze damage reports and make recommendations to the executive team on the need for disaster declaration. It notifies all disaster recovery teams with concurrence from the executive team. Once recovery has begun, this team coordinates all internal DIS recovery activities and monitors progress. It schedules DIS personnel for appropriate support activities and serves as the focal point for all technical and operational questions posed by Customers during the recovery process.

This team has a key role in ongoing disaster recovery preparedness. It is responsible for all planning, testing and maintenance activities necessary to sustain the recovery capability over time.

A number of functional teams report to the disaster management team.

Administrative Support

Administrative support report to the disaster management team and is responsible for record keeping (financial, personnel, materials, etc.) during the period following a disaster. It will support all teams mobilized in the event of disaster at the direction of the disaster management team. It develops expense reporting documentation, prepares insurance claims, supports the preparation of other team reports and assists in the disaster notification process.

Facilities Recovery

This function determines the condition of the computer center and any critical utilities that support its ongoing operation and evaluates the elapsed time before service can be restored. This function coordinates the assessment of damage, compiles inventories of environmental support equipment required to operate the data center, oversees any repairs that are necessary, and oversees the acquisition of new facilities should the original data center be beyond repair. After a disaster, this function ensures that damaged facilities are secure from intrusion and further damage. It conducts a comprehensive assessment of the ongoing security requirements of the data center, ensuring that adequate alarms and monitoring devices are in place.

These findings are to be reported to the management team. Membership in this group will include DIS facilities personnel, operations management, voice and data communications and a number of key equipment and service providers. It is the objective of this function to report within four hours of a disaster event.

Disaster Declaration

This process notifies hot site providers, data archive services, telecommunications utilities and others with an immediate need to know, that DIS will be unable to restore service at its normal computer center within the 72 hour period of *outage tolerance* and that it is mobilizing to restore service from the subscribed hot site locations. This declaration releases funding for travel, transportation and services necessary to support the recovery.

Logistics/Supplies

This team arranges for the transportation of materials, equipment, documentation and personnel, as needed. This includes an ongoing role in the off-site shipment of vital information media, as well as the post-disaster movement of personnel, equipment and backup media to the **Primary** recovery sites on the east coast. It coordinates this activity with the production services team. It will support other post- disaster transportation needs as identified.

This team also coordinates salvaging of forms and other supplies, arranging replenishment as necessary. If supplies are required at the alternate processing sites on the east coast, this team will provide the materials.

.

Human Resources Support

This team will determine the status of personnel affected by the disaster. It will coordinate replacing personnel if necessary and provide support for such activities as medical or disability claims. Where personnel are assigned for long-term work assignments away from the Olympia area, this team will arrange assistance programs.

Communication Services

This team will gather accurate and substantiated information regarding the disaster situation and the DIS response. It will provide notification to employees, customers and the general public on recovery progress via the development of press releases and internal communications. Its charter is to minimize adverse publicity and build public confidence.

Financial Support

This team will ensure access to cash and credit as necessary for the execution of the recovery process by the various DIS disaster recovery teams. Records of all expenditures will be maintained for subsequent insurance, tax and financial reporting purposes.

Internal Systems

DIS has formed a number of internal technical and operational teams to design, test and, in the event of a disaster, execute computing service restoration. These are detailed in the following sections.

Processing Teams

Several Computer Services Division teams within DIS support the restoration of computing services at the subscribed hot site. These teams are directed by Ken Boling, the Disaster Recovery Program Manager, and report up to the disaster management team. All technical, operational and logistical activities associated with the restoration of service are the charter of these teams.

Operating Systems

These teams are responsible for the computing operating systems. There is a UNISYS team, a IBM MVS team, and a IBM-VM team. Each has an obligation to maintain the ongoing recoverability of these systems as they migrate through new releases, new functions, new technologies and new configurations.

Software Support

These teams ensure the availability and functionality of major software utilities in the restored system environment.

Recovery Operations

This team provides operational services at the hot sites.

Production Services

This team arranges the scheduling of critical restoration jobs and initiates normal production schedules when appropriate.

This team ships disaster recovery copies of data to off site storage on an established schedule and arranges transport of this data to the appropriate hot site location. Steps are taken to ensure that two copies of critical data are available and handled separately so that the risk of the loss of this critical asset is mitigated. This team coordinates its activities with the transportation support team.

This team arranges for the production of critical output and its distribution to appropriate recipients.

Network Teams

Two major Telecommunications Services Division teams within DIS support the restoration of telecommunications services. All technical and logistical activities associated with the restoration of needed service are the charter of these teams.

Data Network Recovery

This team restores data network service to the restored computer operations at the east coast hot sites. This charter includes the design, testing, and in the event of disaster, the execution of a data network switching process for both the remotely connected and locally linked end users of the DIS computing platforms (UNISYS and IBM). It will recover local and long-distance data service and participate in any teams formed for cold site occupancy at the east coast disaster recovery service bureaus, site re-occupancy at the home DIS data center, and site restoration at the home DIS data center or site construction, should a new DIS data center be necessary.

Voice Communications

This team will provide local and long-distance voice communications to support the restored operation at the east coast hot sites. This includes access to the restored UNISYS operation, the restored IBM operations and those locations where other DIS personnel have been temporarily located, if necessary, during site restoration and/or construction activities.

THIS PAGE IS INTENTIONALLY LEFT BLANK

IV. Data Backup and Restoration

Purpose

Electronic data is the single most valuable asset in DIS data centers. While disaster-damaged equipment can be replaced with new computers and facilities can be restored or reconstructed, DIS system control data and customer agency electronic information can not be obtained from *any* outside source. It is unique, volatile and irreplaceable. It **must** be protected.

As owner and operator of the UNISYS and IBM processing environments and as custodian of the customer agency data created, updated and maintained therein, DIS is leading the project to design and implement a comprehensive data disaster protection program. While the UNISYS and IBM approaches will be somewhat different at the outset based on historical relationships between DIS and these Customers, it is our intent to implement a process whereby DIS will be accountable for system and control data recoverability and Customers will have full responsibility for the recoverability of the applications and data they own.

The purpose of this data backup and restoration program is to ensure that system and vital application data (to be detailed in the following sections) will be captured regularly and shipped off premises to a protected location so that it will be available in the event of a catastrophe at the DIS data center.

The DIS portion of this process is now fully implemented. **This data is created solely for disaster recovery purposes and is not available for day-to-day production data re-creation purposes**[2]. The data is shipped in sealed tape transportation containers to a professional data archive service outside the Olympia area.

As a double protection, DIS will maintain two complete generations of its data off site and ship these separately to the east coast recovery centers to ensure that an image of critical data will always be obtainable. These generations will be the current generation (weekly cycle) and the next most recent ("minus one") generation.

The DIS portion of the data backup process requires no action on the part of the customer agency except for the review and validation of the restored system environment. Validation opportunities will be provided periodically; a comprehensive disaster recovery demonstration with DIS and customer participation will be conducted at least annually.

DIS will work with customer agencies to determine what **additional** data backup steps or methods are necessary to restore Customer application data to proper production status. **The execution of these steps and the associated off premises tape shipment will be the sole responsibility of the customer agency.** DIS, as custodian for the customers' data, will offer backup and recovery tools, training, production services support, operational tape handling and output service disaster shipment administration at the request of the customer agency for a fee.

[2] Data archived off premises for any purpose other than disaster recovery is out of the scope of this program.

Approach

DIS assumes the responsibility for the capture and ongoing availability of the standard system disaster recovery data image. Similar approaches will be taken for the UNISYS and IBM environment with necessary variations to accommodate the technical differences of the two. Customers of the IBM and UNISYS processors should read the sections that follow which are devoted to a description of these diverse environments. DIS will offer technical and operational support where feasible and as contracted by its customers.

UNISYS Environment

DIS Role and Responsibilities

DIS assumes the responsibility to backup the UNISYS operating environment, including the system software, system utilities, database managers and necessary tables and indices to restore the computing system at the recovery hot site in Warminster, Pennsylvania.

The operating system, or EXEC, is backed up onto tape in "boot"-able format whenever a change is made in:

- The EXEC version
- The DIS UNISYS hardware configuration, or
- The Sungard Recovery Services (hot site) UNISYS hardware configuration.

The backup tape is shipped directly to Sungard where it remains until a new EXEC boot tape is produced in response to changes, as outlined above. Should a disaster be declared, this tape will be loaded on the recovery hardware immediately to begin the UNISYS restoration process.

Each Tuesday evening, system control software, utility programs, real time transaction programs and screens in the shared mass storage pool are backed up using the system utilities, TIP and FURPUR, in the following procedures:

- LIBSAVE
- LOCALSAVE
- TIPSAVE[3]

No user application programs or data are included in this weekly backup. Only system support removable disk volumes are included

The backup tapes are shipped off premises on Wednesday of each week to a professional electronic media archive location, where they remain for two weeks and then are returned to DIS for scratch use. Should a disaster be declared, these weekly backup tapes are shipped immediately to Sungard Recovery Services for use in the UNISYS system restoration process. After the EXEC tape has been loaded and the system booted, these tapes are used to restore the system[4] portion of the mass storage space using the following procedures:

- LIBLOAD
- LOCALOAD
- TIPLOAD

[3] TIPSAVE includes the on-line executable transactions program libraries. These contain agency programs but are included because of the special registration of the files which allows the transactions to be loaded when a user calls for them. Also included are the agency sets of screen files maintained in TIP screen and password files by the Display Processing System (DPS). Although end user products, these are held and maintained by system processors and are saved during TIPSAVEs.

[4] Note that some of the system data is on shared storage, some on removable storage.

The development UNISYS system is out of the scope of this program. Any programs or data resident there will not be recovered at the hot site. Customers must assess their need for data on this system and protect it as they see fit.

Mapper

The "Maintaining, Preparing, and Producing Executive Reports," or MAPPER, utility is used by all UNISYS based customer agencies and DIS assumes major responsibility for the restoration of the **production** MAPPER facility in the event of a disaster. OFISLINK is not included in the disaster recovery restoration process.

Separate disk space has been assigned to MAPPER functions. Data from MAPPER disk files is compacted and off-loaded to tape each evening at approximately 12:00 AM. This tape data is maintained on premises and may be recalled to the MAPPER disk packs, as needed.

On Wednesday, the daily tape operational backup data is consolidated on cartridge tape and shipped off premises to a professional data vaulting service. This data is for disaster recovery purposes.

When a disaster test is conducted or should a disaster be declared, MAPPER backup tape cartridges are shipped to the east coast recovery center. In the restoration processes, the MAPPER utility capability is restored after EXEC is booted, and the load functions (LIBLOAD, LOCALOAD and TIPLOAD) are executed by DIS personnel, as described above. The backup data on tape cartridges will be re-loaded onto the assigned MAPPER disks.

MAPPER should be restored in three to four hours after the restore process begins. Access to the restored system will not be provided until other restore activities have completed (*e.g.*, STAR, tape management system restores, the various customer agency DMS restores and the activation of the Communication Management System, or CMS).

UNISYS Storage Management

Dedicated Mass Storage Files

DIS is responsible for providing the dedicated mass storage capacity necessary for recovery of all production database files registered under TIP recovery. DIS will re-catalogue and allocate these files at the hot-site, then register them with TIP, such that they are ready for database reload procedures. Special word-addressable files are identified and a list of those files is backed up via the shared mass storage routines described in the next section.

Any customer files on dedicated mass storage which are not registered with TIP, and are considered to be mission-critical, should be identified for the shared mass storage backup process, since they will not be recovered as such on dedicated mass storage at the hot-site. All dedicated disk pack-ids used at the hot-site are generic (i.e., REM001,REM002....,REM099) to facilitate the space-allocation and recovery processes. Therefore, no individual dedicated packid will be registered at the hot-site, with the exception of MAPPER and DAILY-PLANIT packs.

Note that all files identified to the shared backup process will be recovered only on shared (fixed) mass storage, regardless of where they exist in the production environment.

Customer Shared Mass Storage Files

DIS will be responsible for creating disaster recovery backup copies of shared mass storage files (excluding private files), and/or dedicated mass storage application support files (non-database files on removable disk) as identified by the customer.

File Identification :

Each customer (DOL and DSHS) is responsible for maintaining a list of their respective shared mass storage files and catalogued tape files which they consider to be mission-critical, and are to be restored at the hot-site by DIS in their recovery procedures. These lists will be maintained on-line on the Production host, using the following file names and formats:

MDOL*DISASTER.DR/DOL-SMS for DOL shared mass storage files
MDOL*DISASTER.DR/DOL-TAPE for DOL catalogued tape file names

SHS*DISASTER.DR/SHS-SMS for DSHS shared mass storage files
SHS*DISASTER.DR/SHS-TAPE for DSHS catalogued tape file names

The format required is

QQQQQQQQQQQ*FFFFFFFFFFFF(CCC).

or fully qualified filename, including file-cycle (F-cycle) number, ended by a period. Relative F-cycle numbers are allowed so that all needed cycles may be included in the recovery process.

Backup schedule

A complete backup of all files the customer has identified on each list is performed once weekly on Sundays, following the normal daily save processing. Catalogued tape file names (MFD items only) are backed up on a daily basis. An incremental backup of shared mass storage files is performed Monday through Saturday following the normal daily save. Output backup tapes are sent off-site on a daily basis for a three-week cycle.

Recovery process

A list of daily backup tapes is sent off-site with the output backup tapes. The recovery is performed using the latest backup tape numbers for input first, then regressing each day until the full weekly set is read in. This is done so that the most current backup is recovered.

Customer Role and Responsibilities

DIS' Unisys Customers are responsible for the protection of their own application programs, databases and other production file structures.

Disk-based application programs (source code, executable on-line transactions and batch programs), tables and application utilities, DMS databases, non-database application data files on disk (whether in shared mass storage or in "removable" volumes) and very large **tape resident** data files are **owned and under the sole protection of the customer, except that DIS will be responsible for creating disaster recovery backup copies of shared mass storage files (excluding private files), and/or dedicated mass storage application support files (non-database files on removable disk) as identified to the Unisys Storage Management Section** Identification will be through maintenance of a list of these mission-critical files. This list must be provided to DIS in text (symbolic) format on the production UNISYS host. The listed files will be backed up on a daily basis via the FAS process as described in the above section.[5]

Otherwise, the customer can create their own shared mass storage file backups through a combination of DMS database utilities, the FURPUR file copy utility and customer developed programs. Comparable programs must be used in the restoration of this data.

Customer agencies are responsible to review all the electronic data they maintain at the DIS UNISYS data center and to make necessary disaster backup copies of vital data. These backups should be at appropriate synchronization points within the application cycle. It must be assumed at this time that no UNISYS data center resident data will be available for disaster recovery purposes. It is recommended that Customer backup tapes be stored off data center and customer agency premises, preferably at the professional data archive location under contract by the State (and used by DIS for all of its disaster recovery backup tape storage). Customer Agencies should make arrangements for disaster backup tapes to be shipped to the recovery hot site in Pennsylvania immediately after a DIS disaster is declared.

To facilitate timely application and data restoration, the customer agencies should develop, test and maintain recovery job schedules to load backup data onto disk (shared mass storage or removable volumes) at the hot site. These restoration schedules should also be backed up onto tape for post-disaster accessibility.

DMS Databases

DIS uses UDSC/DMS2200 system software on the Unisys platform. Because of the large size of their DMS databases, backups have been divided into logically related functional recovery units which are backed up at least once each week. The recovery unit backups are distributed throughout the week based on application demands, as well as operational performance and workload guidelines.

[5] With the exceptions previously listed under TIPSAVE processing which are backed up by DIS personnel.

Weekly backups of the various recovery units are scheduled by customer agency production control personnel who forward these schedules to DIS production control and operations for execution and physical tape handling at the data center. Customer agency designated personnel collect this data from the DIS data center and remove it to a customer agency selected location for protection. It is recommended that the professional electronic media data vaulting firm be used for both the collection and storage of this data.

Each day separate audit trail tapes are collected. When full, a new audit trail tape is mounted and the completed one is set aside for periodic collection by customer agency couriers who remove the audit trail tapes from the DIS premises to customer agency office space. Within each customer agency's audit trail tape all of their database transactions accepted during the period that the Audit Trail tape is being written will be captured.

These audit trail tapes may be used to restore DMS databases to currency using **LONG RECOVERY** processing in the event of a disk or other database problem, as may happen during normal operation. They may also be used in the event of a disaster to bring weekly database backups to transactional currency to within a few hours of the disaster. The customer agencies must devise an approach to deal with transactions between the disaster and the time of the most recent shipment of the Audit Trail tapes off premises.

In general, a complete customer agency backup cycle should be viewed as one complete week's set of recovery unit backup tapes **in combination with** all audit trail tapes shipped off premises during the current week. Applications that have longer or irregular cycles may require a unique backup cycle and handling process, as determined by the customer agencies.

For disaster recovery purposes, it is highly recommended that two complete cycles (current and next most current), be maintained off premises for recovery accessibility. Both the weekly recovery unit backups and daily accumulation of audit trail tapes are necessary to bring the database to near pre-disaster currency. These should be handled and shipped separately to protect the customer agency from a total loss of this vital asset. Such arrangements may be made directly with the professional archivist with cooperation from DIS personnel.

When the database backups arrive at the recovery center and the UNISYS operating environment has been recovered, customer agency personnel can submit recovery schedules to restore the databases, first from the weekly backup tapes and then from the daily audit trail tapes. It is the intention of DIS that our customers will be able to start their database reloads prior to the 72-hour recovery period. The customer should ascertain at what point the data restoration is complete and synchronized with any related database structures and/or dependent application program cycles. DIS will provide periodic (at least annual) opportunities for customers to test their recoverability at the hot site

IMPORTANT NOTE: Unisys based customer agencies are actively involved in the data and application restoration process at the east coast hot site in Warminster, PA. These customers should budget one to two trips to Pennsylvania each year for their technical support personnel to participate in recovery testing.

Source Code, Executable Programs and Other Disk Data

As previously stated under Customer Roles and Responsibilities, with the exception of "hot-site only" mission-critical identified files, the customer agencies are responsible to create disaster copies of their application source, on-line transaction programs and batch programs, whether they are resident on shared mass storage or on customer agency owned removable disks[6]. The backup cycle should be based on the frequency of change to these objects. For any application tables or indices that are volatile, regular scheduled backups are recommended.

Customer agency production application data on disk media that is not within one of the DMS/UDSC database structures must be identified, assessed for recovery priority/value and, if deemed necessary, identified to DIS as mission-critical for FAS backups so they may be captured on disaster backup tapes. Such backup tapes will be stored off-premises under DIS provisions. Arrangements will also be made for their shipment to the recovery hot site for restoration in the event of a disaster. Recovery procedures and schedules for this type of data are required, as well as methods to determine accuracy and production readiness.

Tape Data

Production application data that is maintained exclusively on tape presents special logistical challenges in disaster recovery planning. The customer has two **primary** options:

- Duplicate the data onto disaster backup copies of the tape, or
- Select an earlier version of the data for use in event of a disaster.

The first option can be costly in terms of processing cycles, extra tape, manpower and equipment to execute the duplication. It may also be difficult to accomplish within existing production schedules.

The second option usually means that the "next most recent" copy of the file is stored off premises. It requires the customer agency to devise a mechanism to recapture or recreate the data lost between the current data copy (what would have been input to the next application cycle but is presumed to have been lost or made inaccessible in the DIS data center disaster) and the "minus one" generation copy that is available for recovery.

Customer Agencies are responsible to determine which approach, if either, is best suited to its recovery requirements and to implement a backup process to meet its needs.

[6] A note to remember is that some customers may have **Production Data** (run streams), on the **Development System** and it will be the customers responsibility to make sure this data is properly recovered.

Job Scheduler - Daily Planit

In the event of a disaster, job run sheets will be impossible to handle. Therefore all production jobs should be included in the Unisys job scheduler (**DAILY PLANIT**). To get more information or to schedule your jobs in Daily Planit, please contact Robert Kinzie, 902-3193, OV ID: RK

OFFSITE Storage of Tapes

Customer agencies that create additional disaster recovery backup copies, outside the normal DIS process, are responsible for the off-siting of these tapes to an off-premises storage facility. DIS currently contracts to DataBase Corporation for the off-siting, storage and shipment to hot sites of their disaster recovery and archived data. There are a number of other state agencies that are utilizing the same contract to store their data. Please contact DIS Tape Services, 902-3200, for information regarding what process DIS uses for off-siting tapes and for the correct address of the IBM and Unisys hot sites. You will need to know this information to insure that your disaster recovery tapes are handled and shipped similar to the DIS process.

IBM Environment

DIS Role and Responsibilities

DIS assumes responsibility for executing the standard, baseline disaster recovery data backup and restoration procedures outlined in the following sub-sections. In addition, DIS will maintain the ability, over time, to recreate the MVS and VM operating environments that are in production in the DIS data center.

Ultimately, DIS believes that the customer is the sole arbiter of what customer agency applications or data need disaster recovery protection. On an interim basis, until customer agencies have the opportunity to evaluate their individual requirements and implement necessary backup processes, DIS has devised a **TEMPORARY** process to capture changed production data. Weekly backups of all disk volumes are augmented by daily changed data collection.

This process is intended to minimize the customer's exposure to loss of data after a disaster and to minimize the re-entry of data lost between data backup and the disaster occurrence. For example, if a disaster occurs after 12:00 noon on Thursday, customers should expect that data from the previous evening (Wednesday) will automatically be restored by the DIS disaster recovery teams. If the disaster occurs before noon on Thursday, data from two evenings before (Tuesday) will be restored. The customer agency should therefore assume that as much as two days of data may be lost and act accordingly.

Customer agencies are cautioned to carefully evaluate the method and timing of these backups and **substitute** a customer agency disaster backup process at valid synchronization points within its individual application cycles. The DIS backup methodology is performing full volume based backups, which is the backup of all volumes rather than specific groups (application data) of data. For more detailed explanation see section **"Data backup and restoration /IBM Environment/MVS Platform.** As customer agencies implement their own application program and data backup program, DIS will suspend its temporary application program and data backups. **DIS will terminate all full volume based temporary backups of customer data by the end of fiscal year 1997 .**

Data Capture and Vaulting

Using the Vault Management System (VMS) functions of the Tape Management System (TMS) utility acquired from Computer Associates, DIS manages the following off-site vaults of data:

Description of the types of vaults:

Slotted vaults are allotted a defined space and the Vault Management System assigns a slot number in its process, whether it is used or not. The tape media is then put in that assigned slot.

Non-Slotted vaults are usually containers. The tape media is kept in locked containers and shipped off premises; a return date is indicated for the container.

Vaults 1--3:

1. (**DR1**) is sent off site to an east coast data vaulting service for 16 days and kept in DIS locked containers. This contains CMC **(VTAM Communications)** machine operating system and starter system data needed in the first few hours of the IBM restoration process. This data is created on Sunday using the Full Volume Dump function .

2. (**DR2**) is sent off site within the State of Washington for 16 days and kept in a slotted vault. This vault contains the following kind of data:

    A) It contains Full Volume Dump copies of selected DIS disk volumes and are created each Sunday.

    B) It contains a complete off-line logical image copy of all ADABAS databases created using ADABAS utilities. It is created at the end of the weekend before on-line system start early Monday morning.

    C) It contains SAMS:Disk(DMS/OS) backups captured from permanent production storage (UNIT=PRIM).Two programmed passes are made through the volumes seeking modified files each night, Monday through Sunday. This data has a 28 day cycle.

    D) It contains SAMS:Disk(DMS/OS) backups captured from test storage (UNIT=TEST) Monday through Sunday. This data has a 28 day cycle.

    E) It contains ADABAS transaction Protection Logs. This data is used to restore transactions entered since the weekly **ADABAS** image was captured.

    F) It contains system software backups necessary to data restoration synchronization, as well as disaster recovery start-up process information.

    G) It contains SAMS:Disk(DMS/OS) Archival Data from the permanent production storage (UNIT=PERM). With the exception of generation data sets (gdg), this data has a 2 year cycle. It is **not** automatically restored in the event of a disaster, but is available for both normal operational and disaster recovery purposes.

    H) It contains SAMS:Disk(DMS/OS) Archival Data from the test storage. With the exception of generation data sets (gdg), this data has a 9 month cycle. It is **not** automatically restored in the event of a disaster, but is available for both normal operational and disaster recovery purposes.

    I) It contains Customer Tape Media used for Disaster Recovery purposes. It is expired by the expiration date established for tape media by the customer. Consists of the customer backups of critical applications for disaster recovery purposes. When using this vault,

customers will be required to register unique data set names with Storage Management at 902-3588

Vaults (Nos. 1-2) are for disaster recovery purposes only. The off-site data vaulting service provider is a professional organization that specializes in protecting the information asset of its clients. The physical facility used is outside the Olympia area, adding distance to the other security measures they have in place. This service is available on a fee basis to customers of DIS for their own disaster backup and archive purposes (reference the data vaulting contact in the Disaster Recovery Telephone Directory for further information).

3. **(DR3)** contains data kept for other than disaster recovery purposes such as legal records retention. **CUSTOMER TEST DATA** is also kept in this slotted vault and is not generally sent for disaster recovery purposes. In the event of real extended disaster this tape media will be shipped back east. Also, during any of the bi-yearly exercises, if required, DIS will have this data sent to the hotsites for testing purposes.

Customer Initiated Backup (Proposed)

DIS Storage Management is developing a process to allow customers to initiate the backups of their application data. At a later date instructions on how to use the selected software and the necessary JCL will be provided.

When this is done, the customer agency may insert disaster backup steps within production cycles (on-line or batch) as they deem necessary. ADABAS backups are addressed in another section.

At the recovery hotsite, DIS Storage Management will recover the latest backup copy of the data available. During the transition period, they may require additional verification.

In both the backup and restore, DIS will provide training classes to insure that our customers understand this process.

The DIS backup service will function as follows: The customer agency will decide when they wish to perform their backup process. The Customer will implement their backup, at which time the specified data will be copied from designated files to compressed disk file. Once this backup process is complete, the customer is no longer responsible for any further tasks. At a prescribed time or threshold, DIS will copy these files from compressed disk to compressed tape. Duplicate tapes will be produced and one copy will be shipped off site and the other will stay on site for any data recovery needs. Customer Agencies will be trained to thoroughly understand this process.

Before these jobs are executed, DIS disaster recovery personnel will have formatted all production disk and restored data catalogs to enable the system to recognize and accurately respond to the restoration request.

Where database structures are to be captured, use of appropriate database manager utilities are recommended.

Off Site Shipment

DIS personnel currently pull the tapes identified by the Vault Management System and prepare them for off site shipment. Tapes are packed into locked transport containers; necessary documents are prepared and included before the data vaulting service provider arrives at the DIS data center to collect the newly created backup data and to return backup data with an expired retention period. The table below shows the pickup schedule.

OFFSITE SHIPMENT SCHEDULE

DAY	TMS VAULTS
Sunday	DR1/DR2/DR3
Monday	DR2/DR3
Tuesday	DR2/DR3
Wednesday	DR2/DR3
Thursday	DR2/DR3
Friday	DR2/DR3
Saturday	DR2/DR3

Customer agency- registered VMS off-site vaulting needs to fit in with one of the existing off site shipment schedules . Customer data for disaster recovery purposes will be put in vault DR2 which will be sent off site seven days a week.

MVS Platforms

Different types of data require different handling approaches, as described below.

1. System and Utility Data

   Operating system data is captured weekly or whenever a significant upgrade or corrective maintenance release has been applied. Full system volumes are dumped with FDR for rapid restoration. Records are maintained of any unique system parameters or start-up options.

   Critical to system and data restoration is the synchronization of system and data catalogs. Softwork's *The Catalog Solution* utilities are used in conjunction with Computer Associates' *Tape Management System* features to ensure this synchronization. The following steps are executed at the recovery hot site:

   - Full volume restoration of all system volumes
   - Restoration of all system catalogs
   - Restoration of the *Tape Management System* catalogs (including *VMS*)
   - Restoration of all system critical datasets (tables, programs, pointers)
   - Preparation of all customer disk volumes with volume labels, volume table of contents (VTOCs), Volume VSAM Data Set directory (VVDSs) and indices.

   This process is the sole responsibility of DIS. Tapes containing MVS and data network operating system are shipped whenever a major hardware configuration change occurs at DIS, at the IBM Business Recovery Services Center in Gaithersburg, Maryland, or when DIS implements a major software upgrade. These tapes are always ready for load at the hot site, so that the CMC (VTAM Communications) MVS operating system and data network restoration may begin immediately when a disaster is declared. Other system and related backup tapes are shipped from the off-site vault to the east coast for load after the base operating environment has been restored.

2. VSAM, FOCUS and other Production File Structures

   Each week, a complete full-volume copy is taken of volumes containing this data . It is shipped off site for disaster recovery purposes. A separate process is executed to provide a backup copy of this data for normal operational purposes.

   In addition, each night the SAMS:Disk (DMS/OS) software component has been set up to selectively back up individual data sets (except ADABAS or temporary files) that have changed or been created since the last cycle. To improve the likelihood that all data is current, SAMS:Disk has been instructed to pass through all volumes twice before 7:00 AM to create images of new and changed data. SAMS:Disk creates two copies on cartridge tape. One set is maintained on site; the other is shipped off site for disaster recovery purposes.

Customer agencies should recognize that these nightly backups will be taken when most CICS on-line systems and applications are inactive or at minimum transaction levels. Batch processing, however, may be ongoing during this period. **It is possible that SAMS:Disk created copies of new or changed data may not adequately reflect necessary batch application cycle synchronization points. This is especially likely in applications with multiple batch jobs or applications that share data sets with other applications.**

This backup process is to be executed on an interim basis only. DIS recognizes that this data may not be properly synchronized for Customer Applications and not result in a "production ready" data restoration. It is the responsibility of the customer agency to investigate its own application program and data disaster backup requirements and implement such backup measures as it deems necessary.

Customers should plan to have their own application program and data disaster backup process in place by end of **FY'97**. Opportunities for customer agencies to test and validate their own recovery processes will be provided in periodic disaster recovery exercises. DIS will suspend these interim data backups as customers implement their own.

3. ADABAS Files

For normal operational purposes, the production ADABAS databases are backed up to tape cartridges each day. The Tuesday through Sunday morning backups are done on-line. The Sunday night backup is an off-line backup. The difference is that with the off-line backup, the databases are brought down so that no updates can be processed during creation of the ADABAS backup image. The ADABAS "ADSAV" utility is invoked to create this logical image of the entire database.

A copy is made of these off-line tapes using the ICETOOLS utility of DFSORT. The copy is then sent to off site storage to be used for database recovery at a remote site should a disaster occur at the DIS data center. The Sunday off-line copy becomes the beginning of the current generation (weekly) of ADABAS disaster recovery data. It provides a static **logical** picture of the databases as of the time of the off-line backup.

The protection log files are used to forward recover the ADABAS databases (to recapture transactions that have been entered since the Sunday off-line disaster recovery backup). The protection logs are the accumulations of all transactions that are applied to the databases. These log files are written to disk. When the disk protection log file becomes full, ADABAS automatically switches to a alternate protection log file and copies the log data to tape cartridge. It is the ADABAS "ADARES" utility, employing the PLCOPY function, that switches the protection log files and copies them to tape cartridge.

The ICETOOLS utility is then used to create a disaster recovery copy of the cartridge on a daily basis at 0430 This copy is forwarded to off-site storage to be used exclusively for database recovery at the disaster recovery site. The disk log version and the accumulated ADARES-created tape backup copies remain on

premises for any normal operational need to restore ADABAS transactions at the DIS data center.

The IBM utility IEFBR14 is executed to allocate and catalog the ADABAS database files on the disk volumes provided by the IBM Business Recovery Services Center. After this utility is executed, the recovery of the database at the remote recovery site is done using ADABAS utilities. The ADABAS utility "ADAFRM" is used to format the database storage in the required ADABAS format.

The RESTORE function of the ADABAS utility "ADASAV" is then used to load the databases from the off-site off-line full logical image copy of the backups created from the Sunday backup. Finally, the REGENERATE function of the ADABAS utility "ADARES" is executed to restore the daily copies of the protection log information to bring the databases current (forward from the Monday backup) to the day before the outage.

IMPORTANT NOTE: It is important to know that with the exception of the DSHS databases, DIS Database Services will backup all of the customer's databases and make offsite copies each Sunday night. We will also make offsite copies of the database protection logs (before and after update images) daily. Depending on when a disaster is declared, we probably will not be able t recover a customer's database to the same exact status at the recovery site that they had at DIS at the time the disaster is declared, due to the timing of pickups of the offsite copies at DIS.

You may want to consider this when you put together your agency's disaster recovery plans. Agency ownership of this process will ensure that their data is captured at appropriate points in the application cycle to enable prompt and accurate data restoration and resumption of production processing.

VM Platform

As with MVS, DIS is responsible for recreating the production VM platform in the event of a disaster. OFFICE/VISION, or PROFS, electronic mail system data backup and restoration is also within its charter. Should the Customer Agency wish additional backup and recovery services than those outlined below, this can be arranged under contract with DIS.

The VM Backup Process

1. System Backup

   A number of operational backups are taken of the VM environment. These are available to recover data under normal operating circumstances. For disaster recovery purposes, the VM operating system, including the **Primary** and alternate system residence volumes, are backed up using the DDR/XA utility each Monday evening and shipped off premises on Friday. This data is not volatile and, except in the circumstance of a system upgrade where extra backups are taken, there is no concern of loss of data from a weekly backup.

2. CMS Data Backup

   The CMS files represent more than 90% of the VM data files. These are full-volume dumped, in duplicate with twin output tapes, each Tuesday evening. These backups are taken with VMBACKUP and one copy is shipped off premises for disaster recovery purposes each Friday. Daily changed data tapes are taken but are available for operational backup purposes only.

3. Spool Data Backup

   The SPOOL files containing tickler files and system data areas are full volume dumped, in duplicate with twin output tapes, each Tuesday. These backups are taken with VMSPOOL (or CMS SPTAPE commands). In addition, daily incremental files of changed data are taken six days each week. On Wednesday, these incremental backups are consolidated into two disaster backup tapes. On Friday, a full volume dump copy and the consolidated incrementals are shipped off premises for disaster recovery purposes.

4. Page Data

   This is temporary data and not backed up by DIS.

5. User Data

   User data may be protected using the VMARCHIVE utility. The user submitting such a backup should also send an OFFICE/VISION note to the VMIADMIN userid requesting that the output tape(s) be off sited at the disaster recovery vault for the retention period desired. **There is a fee for this vaulting service.**

   For VM user files that a customer agency needs to back up on a regular, cyclical basis, the customer agency should request that DIS establish a periodic

VMBACKUP process for that data. **This is also a fee based service.**

6. Tape Management

   VMTAPE is the VM tape manager. All disaster recovery tapes are catalogued by VMTAPE. At present, these volumes are cross-logged in a PC-based tracking system for clerical administration and billing purposes, but it is intended that this record keeping be transferred to the IBM Vault Management System. VMTAPE is also backed up to tape for disaster recovery purposes, although in an emergency, it is possible to use backup tapes without access to VMTAPE. This data can be rebuilt from VMBACKUP data.

   System backup tapes have volume serial numbers in the TAP### format.
   User and other tape backups have volume serial numbers in the VA#### format.

The VM Restore Process

The steps below outline the restore process that has been established for the VM computing environment at the east coast recovery site.

1. System Restoration

   System data is restored from tape at the east coast recovery center in stand- alone mode using DDR/XA. The page volumes are formatted in stand-alone processing mode using the IPL/DSF tape. When this is complete, the DIS VM/ESA operating system is initialized. Follow-on forward recovery of data files is done using VMBACKUP changed data files (see below).

2. Data Restoration

   After the VMTAPE and VMBACKUP control files are restored and verified, data restoration proceeds. CMS data that was backed up in the weekly disaster recovery backup tape is restored using VMBACKUP. Spool volumes are restored using VMSPOOL.

   Recovery of specific user-created backup files may then be restored using VMBACKUP or VMARCHIVE, as is appropriate to the backup data.

Customer Responsibilities

While DIS serves as custodian, it is the customer agency that *owns* production application data. For many customer agencies, it is a **vital** asset that must be protected against all contingencies. For this reason, it is the customer agency alone that can certify that the data backup and restoration process devised by DIS will prepare the customer agency to continue its automated functions and processes after a disaster.

Opportunities will be provided for each customer agency to participate in disaster recovery exercises. These will be set up to enable customer agency representatives to sign onto the restored system and enter transactions. Batch applications can also be executed to validate that critical data values and totals have been successfully recreated.

Prioritization of Systems

In beginning disaster recovery planning for the customer agency, it is recommended that the customer agency first inventory its automated application portfolio and determine the restoration priority of each. What is the cost to the customer agency when this application is not available? Will it lose revenues, risk law suit, harm the citizens of the state, etc.? How long can the customer agency tolerate an outage of that system? Are there times of the week, month or year when system restoration is more urgent than at others?

The findings from the *Business Impact Analysis Final Report, table 3*, conducted by DIS and the customer agencies, are a suggested starting point for this internal customer agency evaluation. When applications have been prioritized, they should be prepared in priority sequence for disaster recoverability. This report is available from DIS, upon request.

Technical System Analysis

Each application system should be evaluated from a technical perspective. Here are some of the questions that should be answered:

- What data structures are involved?
- What tools exist to back up and restore data?
- How many files are involved?
- How are they inter-dependent?
- What are the appropriate points in the application cycle to backup data?
- What transaction volumes do we process?
- Can we re-enter these manually if they are not in the disaster backup copy?
- Is this application system dependent on any other system or database?
- Are there equipment, personnel or materials that are critical to the restoration and continued processing of the application system?
- Is the data shared across applications?

In investigating these issues, the customer agency will begin to determine its individual application data backup requirements and schedule copies at more appropriate points in its production cycles than those now generated by the *interim* DIS baseline disaster recovery backup process.

Please refer to the Telephone Directory at the end of this guide for contacts to DIS support specialists who can provide information on specific data backup questions.

Creating Independent Customer Agency Data/File Disaster Backup Images (IBM/MVS only)

Customers may choose to establish a disaster recovery system that is different then the one recommended by DIS. For these customers, the following procedures are outlined.

1. Define a unique data set pattern for this application's backup data.

2. Determine which type of vaulting (archive or disaster recovery only) is needed and what retention period is appropriate. Storage Management recommends that the data be taken once a week and that three generations be maintained. This corresponds to the approach being taken for other disaster recovery data.

   Slotted vaults are allotted a defined space and the Vault Management System assigns a slot number in its process, whether it is used or not. The tape media is then put in that assigned slot.

   Non-Slotted vaults are usually containers. The tape media is kept in locked containers and shipped off premises; a return date is indicated for the container.

3. Contact the DIS IBM Storage Management Group to define a VMS vault and your **exclusive** data set pattern.

4. Begin taking backup copies to tape, using whatever utilities are appropriate to your application and data structure. Plan to use this same utility in restoring data after a disaster.

5. The IBM Storage Management Group will run a batch job each day to identify all VMS tapes that are to be collected and shipped off premises. They will be placed in the pre-defined vault and rotated according to the retention period specified. These tapes will be shipped to the recovery site in the event of a disaster. The customer agency must develop job streams to restore this data.

6. When VMS recognizes that an expiration date has been reached on a disaster recovery tape, it will return the tape from the off-premises vault to the main data center tape library for scratch.

7. Tape that is stored off premises for disaster recovery purposes following the mechanisms described herein will automatically be shipped to the east coast recovery hot sites for full disaster recovery tests and in the event that a disaster is declared.

8. After the MVS system is recovered, each customer using this process will be responsible for recovering their data. Plan to use this same utility in restoring data after a disaster.

9 Customer agencies who require data images in addition to the above described process, will be required to make their own arrangements with the DIS off-site vendor, DataBase, for off-siting and shipping of the tapes. They also need to use their own tapes.

Tape Data

Production application data that is maintained exclusively on tape presents special logistical challenges in disaster recovery planning. The customer has two **primary** options:

- Duplicate the data onto disaster backup copies of the tape, or
- Select an earlier version of the data for use in event of a disaster.

The first option can be costly in terms of processing cycles, extra tape, manpower and equipment to execute the duplication. It may also be difficult to accomplish within existing production schedules.

The second option usually means that the "next most recent" copy of the file is stored off premises. It requires the customer agency to devise a mechanism to recapture or recreate the data lost between the current data copy (what would have been input to the next application cycle but is presumed to have been lost or made inaccessible in the DIS data center disaster) and the "minus one" generation copy that is available for recovery.

It is the responsibility of the customer agency to determine which approach, if either, is best suited to its recovery requirements and to implement a backup process to meet its needs.

Job Scheduler - CA-7

In the event of a disaster, job run sheets will be virtually impossible to handle. Therefore all production jobs should be included in the IBM job scheduler (CA-7). To get more information or to schedule your jobs in CA-7, please contact Robert Kinzie - 902-3192 or Mike Stein - 902-3219

OFFSITE Storage of Tapes

Customer agencies that create additional disaster recovery backup copies outside the normal DIS process are responsible for the off-siting of these tapes to an approved off-premises storage facility. DIS currently contracts to DataBase Corporation for the off-siting, storage and shipment to hot sites of their disaster recovery and archived data. There are a number of other state agencies that are utilizing the same contract to store their data. Please contact DIS Tape Services, 902-3200, for information regarding what process DIS uses for off-siting tapes and for the correct address of the IBM and Unisys hot sites. You will need to know this information to insure that your disaster recovery tapes are handled and shipped similar to the DIS process.

THIS PAGE IS INTENTIONALLY LEFT BLANK

V. Output Production Services

Print Services

Both the IBM and UNISYS recovery centers have print capability. DIS assumes responsibility to provide the standard forms listed in the table below under the "DIS Forms" column. These will be available for print output in the event of a disaster. Those special forms, if they are identified as part of the Agencies Critical Process listed under the "Customer Agency Forms" column, are the responsibility of the customer agency which must make arrangements for the forms to be available and shipped to the appropriate recovery center. This applies both for recovery testing and actual disaster situations.

Once this table has been reviewed and if you find any forms that you no longer have printed at DIS or you find that forms are missing from the table, please contact the DIS Disaster Recovery Coordinator, Ken Boling 902-3036, and let him know of the changes.

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM	0001		
IBM	0002		
IBM	0003		
IBM	0004		
IBM	0016		
IBM	0021		
IBM	0022		
IBM	0023		
IBM	0026		
IBM	0079		
IBM	0081		
IBM	0120		
IBM	0202		
IBM	0203		
IBM	0215		
IBM	0421		
IBM	0422		
IBM	0605		
IBM	0999		
IBM	7081		
IBM		LEAP-020	0990
IBM			
IBM		Admin. Courts-055	0040
IBM			
IBM		Public Disclosure-082	0349
IBM		"	0350
IBM		"	0351
IBM		"	0352
IBM			
IBM		Sec. State-085	0399
IBM		"	0400

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM		Sec. State-085	0401
IBM		"	0402
IBM		"	0403
IBM		"	0404
IBM		"	0406
IBM		"	0408
IBM		"	0409
IBM		"	0410
IBM		"	0411
IBM		"	0412
IBM		"	0888
IBM			
IBM		State Treasurer-090	0051
IBM		"	0195
IBM		"	0434
IBM			
IBM		State Auditor-095	0060
IBM		"	0061
IBM		"	0196
IBM		Dept. Com/Trade/Econ Development-103	0307
IBM		"	0308
IBM		"	0309
IBM		"	0310
IBM		"	0554
IBM			
IBM		OFM - 105	0121
IBM		"	0175
IBM		"	0600
IBM		"	0601
IBM		"	0603
IBM		"	0611
IBM		"	0991
IBM		Health Care Authority 107	0355
IBM		"	0356
IBM		"	0357
IBM		"	0358
IBM			
IBM			
IBM			
IBM		HRISD -111	0082

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM		HRISD-111	0085
IBM		"	0089
IBM		"	0090
IBM		"	0091
IBM		"	0093
IBM		"	0094
IBM		"	0095
IBM		"	0096
IBM		"	0097
IBM		"	0099
IBM		"	0106
IBM		"	0107
IBM		"	0108
IBM		"	0109
IBM		"	0110
IBM		"	0111
IBM		"	0112
IBM		"	0114
IBM		"	0115
IBM		"	0200
IBM		"	0222
IBM		"	0413
IBM		"	0416
IBM		"	0418
IBM		"	0900
IBM			
IBM		Retirement-124	0146
IBM			0147
IBM			0148
IBM			0149
IBM			0150

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM		Retirement-124	0166
IBM		"	0167
			0169
IBM		"	0170
IBM		"	0171
IBM		"	0172
IBM		"	0173
IBM		"	0245
IBM		"	0320
IBM		"	0429
IBM		"	0430
IBM		"	0444
IBM		"	0448
IBM		"	0462
IBM		"	0465
IBM		"	0506
IBM		"	0507
IBM		"	0508
IBM		"	0515
IBM		"	0518
IBM		"	0569
IBM		"	0584
IBM		"	0662
IBM		"	0663
IBM		"	0664
IBM		"	0665
IBM		"	0961
IBM		"	0963
IBM		"	0965
IBM		Dept. Printing-130	0125
IBM		"	0174

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM		Dept. Revenue-140	0519
IBM		"	0520
IBM		"	0521
IBM		"	0522
IBM		"	0523
IBM		"	0524
IBM		"	0525
IBM		"	0526
IBM		"	0527
IBM		"	0528
IBM		"	0529
IBM		"	0530
IBM		"	0531
IBM		"	0534
IBM		"	0535
IBM		"	0692
IBM		Dept. Revenue-140	0800
IBM			
IBM		Gen. Admin-150	0020
IBM		"	0025
IBM		"	0a93
IBM		"	0131
IBM		"	0132
IBM		"	0210
IBM		Gen. Admin-150	0212
IBM			
IBM		DIS-155	0083
IBM		"	0419
IBM		"	0423
IBM		"	0449
IBM		"	0453

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM		DIS-155	0463
IBM			
IBM		Ins. Comm-160	0230
IBM		"	0231
IBM		"	0234
IBM		Ins. Comm-160	0428
IBM			
IBM		State Board of Accountancy-165	0306
IBM			
IBM		Board of Industrial Ins. Appeal-190	0447
IBM		"	0536
IBM			
IBM		LCB-195	0024
IBM		"	0071
IBM		"	0223
IBM		"	0250
IBM		"	0263
IBM		"	0265
IBM		"	0267
IBM		"	0269
IBM		"	0270
IBM		"	0337
IBM		"	0438
IBM		"	0439
IBM		"	0700
IBM		"	0702
IBM		"	0704
IBM		"	0708
IBM		"	0710
IBM		"	0803
IBM		LCB-195	0890

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM			
IBM			
IBM			
IBM			
IBM		WSP-225	0204
IBM		"	0360
IBM			
IBM		LNI-235	0179
IBM		"	0201
IBM		"	
IBM		"	
IBM		"	
IBM		"	0450
IBM		"	
IBM		"	0452
IBM		"	0568
IBM		"	
IBM		"	
IBM		"	0807
IBM		"	
IBM		"	
IBM		"	
IBM		"	0812
IBM		"	
IBM		"	0814
IBM		"	0815
IBM		LNI235	0906
IBM			
IBM			
IBM			
IBM			

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM			
IBM			
IBM			
IBM			
IBM			
IBM			
IBM		DOL-240	0104
IBM		"	0557
IBM		"	0558
IBM			
IBM		Inder. Sentence Review-250	0273
IBM			
IBM		DSHS-300	0340
IBM		"	0341
IBM		"	0342
IBM		"	0343
IBM		"	0344
IBM		"	0345
IBM		"	0346
IBM		"	0347
IBM		"	0391
IBM		"	0500
IBM		DSHS-300	0980
IBM			
IBM		DOH-303	0360
IBM		"	0361
IBM		"	0362
IBM		"	0363
IBM		"	0364
IBM		DOH-303	0365
IBM			

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM		Dept. Corrections-310	0424
IBM			
IBM		Service for Blind-315	0271
IBM		"	0272
IBM			
IBM		Higher Educ. Coordinating Bd.-343	0348
IBM		"	0730
IBM			
IBM		SPI-350	0205
IBM		"	0537
IBM		"	0538
IBM			
IBM		Evergreen State College-376	0275
IBM			
IBM		Art Commission-387	0930
IBM			
IBM		DOT-405	0224
IBM		"	0225
IBM		"	0226
IBM		"	0325
IBM		"	0338
IBM		"	0339
IBM		"	0555
IBM		Ecology-461	0135
IBM		"	0165
IBM		"	0168

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM			
IBM		Fish/Wildlife-477	0431
IBM		"	0432
IBM		"	0433
IBM		"	0437
IBM		"	0441
IBM		"	0470
IBM		"	0471
IBM		"	0539
IBM		"	0802
IBM		"DNR-490	0279
IBM		"	0280
IBM		"	0281
IBM		"	0436
IBM			0790
IBM		Employment Security-540	0032
IBM		"	0180
IBM		"	0182
IBM		"	0183
IBM		"	0184
IBM		"	0188
IBM		"	0191
IBM			
IBM		"	0666
IBM			
IBM		"	0670
IBM		"	0671

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
IBM		Employment Security-540	0673
IBM		"	0674
IBM		"	0675
IBM		"	0676
IBM		"	0679
IBM		"	0684
IBM		"	0691
IBM		"	0694
IBM		"	0695
IBM			
IBM			
IBM		"	0750
IBM		"	0761
IBM		"	0762
IBM		"	0763
IBM			
IBM		"	0849
IBM		"	0851
IBM			
IBM		Franklin County-811	0774
IBM		"	0775
IBM		"	0776
IBM		"	0777
IBM		"	0778
IBM		"	0920
IBM			
IBM			
IBM			
IBM			
IBM			
IBM			

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
UNISYS		DSHS-300	312
UNISYS		"	313
UNISYS		"	314
UNISYS		"	315
UNISYS		"	316
UNISYS		"	317
UNISYS		"	320
UNISYS		"	321
UNISYS		"	322
UNISYS		"	324
UNISYS		"	325
UNISYS		"	332
UNISYS		"	336
UNISYS		"	351
UNISYS		"	354
UNISYS		"	358
UNISYS		"	359
UNISYS		"	360
UNISYS		"	361
UNISYS		"	369
UNISYS		"	372
UNISYS		"	385
UNISYS		"	416
UNISYS		"	417
UNISYS		"	418
UNISYS		"	419
UNISYS		"	420
UNISYS		"	421
UNISYS		"	422
UNISYS		"	423
UNISYS		DSHS-300	426

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
UNISYS		DSHS-300	427
UNISYS		"	432
UNISYS		"	434
UNISYS		"	436
UNISYS		"	438
UNISYS		"	440
UNISYS		"	442
UNISYS		"	444
UNISYS		"	446
UNISYS		"	448
UNISYS		"	450
UNISYS		"	451
UNISYS		"	452
UNISYS		"	453
UNISYS		"	454
UNISYS		"	455
UNISYS		"	456
UNISYS		"	457
UNISYS		"	458
UNISYS		"	459
UNISYS		"	460
UNISYS		"	461
UNISYS		"	462
UNISYS		"	463
UNISYS		"	464
UNISYS		"	465
UNISYS		"	466
UNISYS		"	467
UNISYS		"	468
UNISYS		"	470
UNISYS		DSHS-300	471

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
UNISYS		DSHS-300	472
UNISYS		"	473
UNISYS		"	474
UNISYS		"	475
UNISYS		"	476
UNISYS		"	477
UNISYS		"	478
UNISYS		"	479
UNISYS		"	480
UNISYS		"	481
UNISYS		"	482
UNISYS		"	483
UNISYS		"	484
UNISYS		"	485
UNISYS		"	486
UNISYS		"	487
UNISYS		"	488
UNISYS		"	489
UNISYS		"	S10
UNISYS		"	S11
UNISYS		"	S12
UNISYS		"	S13
UNISYS		"	S15
UNISYS		"	S16
UNISYS		"	S17
UNISYS		"	S18
UNISYS		"	S19
UNISYS		"	S20
UNISYS		"	S21
UNISYS		"	S22
UNISYS		DSHS-300	S23

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
UNISYS		DSHS-300	S24
UNISYS		"	S32
UNISYS		"	S33
UNISYS		"	S36
UNISYS		"	S37
UNISYS		"	S38
UNISYS		"	994
UNISYS		"	995
UNISYS		"	996
UNISYS			
UNISYS		DOL-240	101
UNISYS		"	108
UNISYS		"	109
UNISYS		"	111
UNISYS		"	114
UNISYS		"	116
UNISYS		"	135
UNISYS		"	137
UNISYS		"	139
UNISYS		"	142
UNISYS		"	143
UNISYS		"	146
UNISYS		"	147
UNISYS		"	149
UNISYS		"	157
UNISYS		"	159
UNISYS		"	164
UNISYS		"	165
UNISYS		"	166
UNISYS		"	168
UNISYS		DOL-240	170

IBM or UNISYS	DIS Forms	Customer Agency Owner(s)	Customer Agency Form(s)
UNISYS		DOL-240	181
UNISYS		"	197
UNISYS		"	203
UNISYS		"	205
UNISYS		"	214
UNISYS		"	215
UNISYS		"	216
UNISYS		"	219
UNISYS		"	220
UNISYS		"	221
UNISYS		"	224
UNISYS		"	250
UNISYS		"	288
UNISYS		"	297
UNISYS		DOL-240	299
UNISYS			
UNISYS			
UNISYS	1412 1 part		
UNISYS	1412 2 part		
UNISYS	LZ Xerox Prt.		
UNISYS			
UNISYS			
UNISYS			
UNISYS			
UNISYS			
UNISYS			
UNISYS			
UNISYS			
UNISYS			
UNISYS			
UNISYS			

Print Services, Cont.

DIS recognizes that there are some logistical difficulties associated with print production and output distribution from east coast recovery centers. Mailing, sorting, collation and other paper handling requirements might be awkward at a great distance away from normal operation. Costs to send trained personnel to handle this process may prove prohibitive. For that reason, DIS has investigated a number of options to provide local print capability for Xerox and S/390 print. Unfortunately there is no local option for the Unisys Impact print:

For UNISYS, the approach is to print all Impact Print at the Sungard hot-site until further notice. This option is being aggressively investigated to determine other ways to provide Impact print for the Unisys Platform.

The Xerox print will be dumped to tape and shipped to the West Coast. DIS is able to drop ship a Xerox printer at a location of their choice and print from there. Some scheduling and throughput limitations would be expected.

For S/390, DIS has created two local alternate print locations. One site is at the Lacey Node and the other is located within the same building that the Seattle Node is located. The approach is to drop ship Impact and Laser printers at either location. Both locations have been pre-wired for this equipment and appropriate Network bandwidth has been provided. Upon a declared disaster declaration, one of these locations would be activated. All customers would be made aware of this location, so that they would be able to make arrangements for the pickup of printed output and warrants. SNAKE tapes would be handled in the same manner. Any customer agency that produces warrants is advised to contact DIS to work out an agreement for this contingency and to make arrangements for testing of the capability.

Microfiche Services

DIS assumes responsibility to save all output that is targeted for microfiche or microfilm production in tape media. It will not automatically be produced in fiche or film in the event of a disaster. Hot site disaster recovery services for microfiche are cost prohibitive.

Customer agencies with a need for microfiche or microfilm production will need to make arrangements for its production **DIS COM Services will provide assistance in locating and arranging this service should it become necessary, but cannot guarantee turnaround times. Please contact Bonnie Beatty for further information, at 902-3191**

Special Forms/Supplies

The responsibility for special print forms is described in the *Print Services* section above. It is recommended that customer agencies review all of the production requirements of their DIS based electronic applications to determine if any other unique

supplies are necessary. Any other special materials or supplies should **not** be assumed.

During the 4th quarter of FY'94, DIS purchased IBM 3900 Laser Printers. This new technology has replaced all of the 3800 Laser Printers. The customer will not have any responsibility to recover the 3900 Electronic Images. This process has been included in the normal system backup process.

The customer agency disaster recovery contact should discuss any other critical resource requirements with DIS. For more information, please contact Bonnie Beatty, Print Services Manager at 902-3191

THIS PAGE IS INTENTIONALLY LEFT BLANK

VI. Customer Interface

Introduction

State customer agencies have been tasked with establishing a comprehensive disaster recovery program by July 1, 1993. Recovery of critical information systems is expected to be a key component of the individual customer agency recovery plans. DIS will work with customer agencies to interface agency plans to the DIS plan, but cannot address customer agency disaster recovery needs beyond the scope of the DIS Disaster Recovery Plan.

DIS Application Brokering maintains a list of private sector consulting services qualified to provide assistance in the development of business resumption strategies.

Customer Agency Disaster Recovery Contacts

DIS will interface with each customer agency through its assigned disaster recovery contact. This will include training and consultation on data backup and off-site tape storage practices, as well as coordination of disaster recovery testing exercises. In the event of a disaster declaration, DIS will work with the disaster recovery contact for each customer agency to expedite recovery activities. An alternate for the contact is required.

Refer to the section entitled **Telephone Directory** section VII, for a list of customer agency disaster recovery contacts.

Disaster Recovery Special Interest Group

DIS , will sponsor the Disaster Recovery Special Interest Group. This will involve monthly sessions for the exchange of technical information, gathering of customer agency requirements and plans, updates on DIS programs and capabilities related to disaster recovery and planning forums for upcoming disaster recovery exercises. Please contact Ken Boling at, 902-3036, for more information, including dates and times for this meeting.

Emergency Communications (1-800 Number)

In the event of an emergency affecting DIS production services, DIS disaster recovery team members will alert the appointed customer agency disaster recovery contact. Status updates and recovery activity coordination will also be via the customer agency disaster recovery contact. In order to assure that contact can be made under a variety of unpredictable circumstances, DIS recommends that the customer agency identify a **Primary** contact and at least one alternate. These personnel should provide **all** of the following:

- Office telephone that is always answered during normal business hours and not subject to power outages (*i.e.*, Centrex telephone service, not electronic key or PBX without power back-up).

- Home telephone
- Home address
- Job title
- Cellular and/or pager number
- Office Mail Stop

DIS has provided a list of current customer agency disaster recovery contacts, refer to section entitled **Telephone Directory** that has been provided by our customer agencies. This list should be reviewed to insure that the appropriate agency contact is listed. If there are any updates to this list, please contact Ken Boling of DIS at 902-3036.

DIS has created a 1-800 Disaster Recovery Hot-Line, that will be used during a disaster. This phone number and instructions will be provided to all DR Customer Contacts. Current information and DIS status will be provided by this 1-800 number.

It is the responsibility of the customer agency disaster recovery contact to establish an internal notification process within the customer agency. **DIS will call only the designated agency disaster recovery contact.**

THIS PAGE IS INTENTIONALLY LEFT BLANK

VII. Telephone Directory

Agency List:

AGENCY LIST: (In order by Agency Number)

AGENCY - 011 - House of Representatives

AGENCY - 012 - Senate

AGENCY - 020 - LEAP Committee

AGENCY - 038 - Legislative Service Center

AGENCY - 047 - Commission on Supreme Courts Report (Reporter of Decisions)

AGENCY - 055 - Office of the Administrator for the Courts

AGENCY - 075 - Office of the Governor

AGENCY - 077 - Energy Office

AGENCY - 082 - Public Disclosure Commission

AGENCY - 085 - Secretary of State - Corporate Division

AGENCY - 090 - State Treasurer

AGENCY - 095 - State Auditor's Office

AGENCY - 100 - Office of the Attorney General

AGENCY - 103 - Department of Community, Trade & Economic Development

AGENCY - 105 GR - Office of Financial Management

AGENCY - 107 - Health Care Authority

AGENCY - 111 - Department of Personnel - HRISD

AGENCY - 116 - Washington State Lottery

AGENCY - 117 - Gambling Commission

AGENCY - 124 - Department of Retirement Systems

AGENCY - 126 - State Investment Board

AGENCY - 130 - Department of Printing

AGENCY - 140 - Department of Revenue

AGENCY - 150 - General Administration

AGENCY - 155 - Department of Information Services

AGENCY - 160 - Office of Insurance Commissioner

AGENCY - 190 - Board of Industrial Insurance Appeals

AGENCY - 195 - Washington State Liquor Control Board

AGENCY - 215 - WUTC

AGENCY - 225 - Washington State Patrol Data Center

AGENCY - 235 - Department of Labor and Industries

AGENCY - 240 - Department of Licensing

AGENCY - 300 - Department of Social and Health Services

AGENCY - 303 - Department of Health

AGENCY - 305 - Agency For Veteran Affairs

AGENCY - 310 - Department of Corrections

AGENCY - 315 - Service for the Blind

AGENCY - 343 - Higher Education Coordinating Board

AGENCY - 350 - Superintendent of Public Instruction

AGENCY - 352 - State Board for Comm & Tech Colleges

AGENCY - 365 - Washington State University

AGENCY - 370 - Eastern Washington University

AGENCY - 375 - Central Washington University

AGENCY - 376 - Evergreen State College

AGENCY - 380 - Western Washington University

AGENCY - 385 - Washington State Library

AGENCY - 405 - Department of Transportation

AGENCY - 461 - Department of Ecology

AGENCY - 465 - Washington State Parks and Recreation Commission

AGENCY - 467 - Interagency Committee for Outdoor Recreation

AGENCY - 477 - Department of Fish & Wildlife

AGENCY - 490 - Department of Natural Resources

AGENCY - 495 - Department of Agriculture

AGENCY - 540 - Employment Security

AGENCY - 678 - Tacoma Community College

AGENCY - 699 - Washington Community and Technical Colleges

AGENCY - 954 - Washington Public Power Supply System

Customer Agency Disaster Recovery Contacts:

AGENCY - 011 - House of Representatives

Primary Contact - Fanette Stewart
Title: Facilities
Office phone number: 360-786-7012

AGENCY - 012 - Senate

Primary Contact - Richard Fisher
Title: Sergeant At Arms
Office phone number: 360-786-7560

Secondary Contact - Steve Lynch
Title: Systems Technician
Office phone number: 360-786-7060

AGENCY - 020 - LEAP Committee

Primary Contact - Bob Fitchitt
Title: Administrator
Office phone number: 360-753-5911

Secondary Contact - Curtis Gilbertson
Title: Applications Consultant
Office number: 360-753-5911

AGENCY - 038 - Legislative Service Center

Primary Contact - Nate Naismith
Title: Manager, Management Support Group
Office phone number: 360-786-7725

Secondary Contact - Larry Watilo
Title: Business Administrator
Office phone number: 360-786-7002

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 055 - Office of the Administrator for the Courts

Primary Contact - Brian Backus
Title: Deputy Director, ISD
Office phone number: 360-753-3365

Secondary Contact - Patty Frost
Title: Technical Support Analyst
Office phone number: 360753-3365

AGENCY - 075 - Office of the Governor

Primary Contact - Lori Jones
Title: CISS
Office phone number: 360-753-4378

Secondary Contact - Jim A. Anderson
Title: Assistant Manager
Office phone number: 360-753-4573

Third Contact - Allen Schmidt
Title: IS Manager
Office phone number: 360-664-3373

AGENCY - 077 - Energy Office

Primary Contact - Jim Squire
Title: CTS2
Office phone number: 360-956-2116

Secondary Contact - Jim Colombo
Title: ITM1
Office phone number: 360-956-2027

AGENCY - 082 - Public Disclosure Commission

Primary Contact - Karen Copeland
Title: Assistant Director
Office phone number: 360-753-1111

Secondary Contact - Malissa Warheit
Title: Executive Director
Office phone number: 360-753-1980

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 085 - Secretary of State - Corporate Division

Primary Contact - Rand Daley
Title: CIC3
Office phone number: 360-753-2524

Secondary Contact - Ellen Myers
Title: Datacomm Tech 1
Office phone number: 360-586-8256

AGENCY - 090 - State Treasurer

Primary Contact - J. Micheal Frost
Title: Project Manager
Office phone number: 360-586-4641

Secondary Contact - Patrick Bohlig
Title: Software Manager
Office phone number: 360-586-2878

AGENCY - 095 - State Auditor's Office

Primary Contact - Roger Brittingham
Title: Assistant Manager
Office phone number: 360-753-3549

Secondary Contact -Susan Smith
Title: CIC2
Office phone number: 360-664-2546

AGENCY - 100 - Office of the Attorney General

Primary Contact - Dave Finnick
Title: Computer Information Consultant.
Office phone number: 360-664-4317

Secondary Contact - Jim Albert
Title: Information Systems Manager
Office phone number: 360-664-0159

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 103 - Department of Community, Trade & Economic Development

Primary Contact - Jackie Jones-Hook
Title: Project Lead
Office phone number: 360-586-4505

Secondary Contact - Steve Armstrong
Title: Information Technology Manager
Office phone number: 360-586-1398

AGENCY - 105 GR - Office of Financial Management

Primary Contact - Lori Jones
Title: CISS
Office phone number: 360-753-4378

Secondary Contact - Jim A. Anderson
Title: Assistant Manager
Office phone number: 360-753-4573

Third Contact - Mike Contris
Title: CISS2
Office phone number: 360-664-3378

Fourth Contact - Allen Schmidt
Title: IS Manager
Office phone number: 360-664-3373

AGENCY - 107 - Health Care Authority

Primary Contact - Marilyn Tucker
Title: Customer Service Manager
Office phone number: 360-923-2851

Secondary Contact - Hieu Ngyen
Title: Manager BHP
Office phone number: 360-923-2840

AGENCY - 111 - Department of Personnel - HRISD

Primary Contact - Gary Maciejewski
Title: Business/Technology Integration Manager
Office phone number: 360-459-6656

Secondary Contact - Aloha Brown
Title: Technical/Production Services Manager
Office phone number: 360-459-6627

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 116 - Washington State Lottery

Primary Contact - Mike Bieker
Title: Information Resources Manager
Office phone number: 360-586-1090

Secondary Contact - Tom Brewer
Title: Assistant Director, Management Services Division
Office phone number: 360-753-1947

AGENCY - 117 - Gambling Commission

Primary Contact - Gerald J. Klein
Title: Computer Analyst/Programmer
Office phone number: 360-438-7654

Secondary Contact - None Given

AGENCY - 124 - Department of Retirement Systems

Primary Contact - Jim Gunn
Title: Prod. Application Manager
Office phone number: 360-753-2530

Secondary Contact - Sharon Megiveron
Title: Disaster Recovery Specialist
Office phone number: 360-586-4584

AGENCY - 126 - State Investment Board

Primary Contact - Tom Edwards
Title: PC/LAN Support
Office phone number: 360-664-8297

Secondary Contact - Jim Lee
Title: Data Systems Manager
Office phone number: 360-664-8295

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 130 - Department of Printing

Primary Contact - Mike Cole
Title: Data Processing
Office phone number: 360-753-6820

Secondary Contact - Mike Hickox
Title: Special Projects/Programming
Office phone number: 360-753-6820

AGENCY - 140 - Department of Revenue

Primary Contact - Carl Schwarmann
Title: Security Administrator
Office phone number: 360-586-6986

Secondary Contact - Carolyn Hoyt
Title: Clerk Typist 3
Office phone number: 360-664-0321

AGENCY - 150 - General Administration

Primary Contact - Ray LeVee
Title: ITM 2
Office phone number: 360-586-3504

Secondary Contact - Don Pohlman
Title: CIC 3
Office phone number: 360-586-2764

AGENCY - 160 - Office of Insurance Commissioner

Primary Contact - Bill Storms
Title: Information Systems Manager
Office phone number: 360-753-7386

Secondary Contact - Hanno Oldenburg
Title: CISS I
Office phone number: 360-586-1006

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 190 - Board of Industrial Insurance Appeals

Primary Contact - Dan Lipp
Title: Information Technology Manager
Office phone number: 360-586-6346

Secondary Contact - Larry Ramsey
Title: Computer Information Consultant
Office phone number: 360-586-6346

AGENCY - 195 - Washington State Liquor Control Board

Primary Contact - Jim Plonski
Title: Operations Manager
Office phone number: 360-753-6345

Secondary Contact - Curt Volland
Title: Data Processing Manager
Office phone number: 360-753-9113

AGENCY - 215 - WUTC

Primary Contact - Bob Klein
Title: Programmer/Analyst
Office phone number: 360-753-3056

Secondary Contact - Mike Kretzler
Title: Information Services Manager
Office phone number: 360-753-3055

AGENCY - 225 - Washington State Patrol Data Center

Primary Contact - Larry M. Wassman
Title: Data Center Manager
Office phone number: 360-586-3561

Secondary Contact - Daniel W. Parsons
Title: Technical Services Manager
Office phone number: 360-586-7562

AGENCY - 235 - Department of Labor and Industries

Primary Contact - Lisa Micheau
Title: Administrative Assistant 2
Pager phone number: 360-923-8041

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 240 - Department of Licensing

Primary Contact - Mike Roberts
Title: Unisys DBA
Office phone number: 360-586-4541

Secondary Contact - Len Devenere
Title: IBM DBA
Office phone number: 360-664-4943

Third Contact - Bob Marlatt
Title: Assistant Director, Info. Svs.
Office phone number: 360-753-6926

AGENCY - 300 - Department of Social and Health Services

Primary Contact - Ken Raupp
Title: ISSD Operations Manager
Office phone number: 360-902-7615

Secondary Contact - Cheryl Chorba
Title: ISSD Production Control Manager
Office phone number: 360-902-7617

Third Contact - Bill Allen
Title: DR Specialist
Office phone number: 360-902-7709

AGENCY - 303 - Department of Health

Primary Contact - Tom Martin
Title: Technical Services Manager
Office phone number: 360-705-6110

Secondary Contact - Tom Harmon
Title: Risk/Emergency Manager
Office phone number: 360-705-6341

AGENCY - 305 - Agency for Veteran Affairs

Primary Contact -Andy Jackson
Office phone number: 360-586-8394

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 310 - Department of Corrections

Primary Contact - Charly Ryman
Title: WAN Administrator 2
Office phone number: 360-753-0140

Secondary Contact - Wayne Wilkes
Title: DCT3 Customer Support
Office phone number: 360-586-8539

Third Contact - Patti March
Title: DCT3 Customer Support
Office phone number: 360-586-8539

AGENCY - 315 - Service for the Blind

Primary Contact - Fay Bronson
Title: Assistant Director
Office phone number: 360-586-1250

Secondary Contact - DSB contracts all services with DIS via ADABAS Natural, CICS, RDS, TSO, etc. DIS should be a primary notification also.

AGENCY - 343 - Higher Education Coordinating Board

Primary Contact - Tom Jons
Title: Director, Information Services
Office phone number: 360-753-7890

Secondary Contact - Tom Bohon
Title: Systems Analyst
Office phone number: 360-753-7891

AGENCY - 350 - Superintendent of Public Instruction

Primary Contact - Bob Patterson
Title: Systems Administrator
Office phone number: 360-664-0368

Secondary Contact - Ed Strozyk
Title: Director, IRM
Office phone number: 360-753-1701

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 352 - State Board for Comm & Tech Colleges

Primary Contact - Mike Scroggins
Title: Information Systems Manager
Office phone number: 360-586-8771

Secondary Contact - Liz Baker
Title: Assistant Director, Operations
Office phone number: 360-753-3670

AGENCY - 365 - Washington State University

Primary Contact - David L. Johnson
Title: Director of Computing
Office phone number: 509-335-3584

Secondary Contact - Jim Haugen
Title: Assistant Director
Office phone number: 509-335-8643

AGENCY - 370 - Eastern Washington University

Primary Contact - Wayne Praeder
Title: Assoc. VP for Information Resources/CIO
Office phone number: 509-359-6915

Secondary Contact - Stephen Davis
Title: Director, Telecommunications Resources
Office phone number: 509-359-6685

AGENCY - 375 - Central Washington University

Primary Contact - James A. Haskett
Title: Director of Information Resources
Office phone number: 509-963-2921

Secondary Contact #1 - Terilee Germain
Title: Systems Manager
Office phone number: 509-963-2946

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 376 - Evergreen State College

Primary Contact - James O. Johnson
Title: Director of Computing and Communications
Office phone number: 360-866-6000 ext. 6238

Secondary Contact - Dale Ard
Title: System Programmer Supervisor
Office phone number: 360-866-6000 ext.6237

AGENCY - 380 - Western Washington University

Primary Contact - Jayne Vaughn
Title: Computer Operations Supervisor
Office phone number: 360-650-2978

Secondary Contact - Richard R. Porter
Title: Director, Administrative Services
Office phone number: 360-650-3502

AGENCY - 405 - Department of Transportation

Primary Contact - MIS Help Desk (Normal Work Hours)
Office phone number: 360-705-7050

Secondary Contact - MIS Computer Operations (Off Hours)
Office phone number: 360-705-7680

Third Contact - Jim McClue
Title: DR Coordinator
Office phone number: 360-705-7696

Fourth Contact - Dennis DeFries
Title: DR Manager
Office phone number: 360-705-7707

AGENCY - 461 - Department of Ecology

Primary Contact - Judy Mattingly
Title: ISS Help Desk
Office phone number: 360-407-6911

Secondary Contact - Sunny Cotey
Title: ISS Operations Manager
Office phone number: 360-407-6586

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 465 - Washington State Parks and Recreation Commission

Primary Contact - Art E. Brown
Title: Information Processing Manager
Office phone number: 360-753-2525

Secondary Contact - Mike Giovanni
Title: CIC 3
Office phone number: 360-586-7007

AGENCY - 467 - Interagency Committee for Outdoor Recreation

Primary Contact - Thelma Smith
Title: Network Administrator
Office phone number: 360-902-3010

Secondary Contact - Debra Wilhelmi
Title: Assistant Director
Office phone number: 360-902-3005

AGENCY - 477 - Department of Fish and Wildlife

Primary Contact - Phil Coates
Title: Chief of Data Management
Office phone number: 360-902-2300

Secondary Contact - Mary Ellen Bradley
Title: ISM2
Office phone number: 360-902-2303

Third Contact - Debbie Howell
Title: CICS
Office phone number: 360-902-2334

AGENCY - 490 - Department of Natural Resources

Primary Contact - Larry Sugerbaker
Title: Manager, Land Information
Office phone number: 360-902-1546

Secondary Contact - Norm Gunther
Title: Manager, Technical Consulting
Office phone number: 360-902-1514

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 495 - Department of Agriculture

Primary Contact - Phillip Maddalosso
Title: Computer Information Consultant II
Office phone number: 360-902-2007

Secondary Contact - James Martinez
Title: Manager, Information Technology
Office phone number: 360-902-2004

AGENCY - 540 - Employment Security

Primary Contact - Diane Vasarkovy
Title: Director, OIS
Office phone number: 360-438-4780

Secondary Contact - Dennis Laine
Title: IT Architect
Office phone number: 360-438-3225

Third Contact - Thomas Bynum
Office phone number: 360-438-4867

Fourth Contact - Carol Lund
Office phone number: 360-438-4725

AGENCY - 678 - Tacoma Community College

Primary Contact - Gary Sigmen
Title: Director of Information Services
Office phone number: 360-566-5007

Customer Agency Disaster Recovery Contacts Continued:

AGENCY - 699 - Washington Community and Technical Colleges

Primary Contact - Wes Morgan
Title: Production Services Manager
Office phone number: 206-803-9737

Secondary Contact - John Lowdon
Title: Systems Support Manager
Office phone number: 206-803-9729

AGENCY - 954 - Washington Public Power Supply System

Primary Contact - Dennis Bailey
Title: Supervisor, Mainframe Services
Office phone number: 509-372-5395

Secondary Contact - Karen Hughes
Title: Lead Computer Operator
Office phone number: 509-372-5276

THIS PAGE IS INTENTIONALLY LEFT BLANK

VIII.Calendar of Events

Fiscal Year 1992 (July 1991 - June 1992)

Exercise Schedule:

DATE	LOCATION	IBM-VM	UNISYS	TSD	LENGTH OF	STATUS
					EXERCISE	&
					AND START	FY' OF
					TIME (Easterr	EXERCISE
					Standard Time)	
Nov. 21	Franklin Lakes NJ	Proof of			8 Hours	Completed / 92
		Concept			0800 Nov.21	
Jan. 17-18	Franklin Lakes NJ	Exercise #1			20 Hours	Completed / 92
					0800, Jan. 17	
Feb. 27	Warminster, PA		Proof of		8 Hours	Completed / 92
			Concept		0800, Feb. 27	

- TSD has been in the process of working with their shared and dedicated network customers in preparing them for the move to the Lacey Network Center. This customer contact will continue throughout FY'94.

Fiscal Year 1993 (July 1992 - June 1993)

Exercise Schedule:

DATE	LOCATION	IBM-VM	UNISYS	TSD	LENGTH OF	STATUS
					EXERCISE	&
					AND START	FY' OF
					TIME (Easterr	EXERCISE
					Standard Time)	
July 21-22	Franklin Lakes NJ	Exercise #2			24 Hours	Completed / 93
					1100, July 21	
Aug. 25-26	Warminster, PA		Exercise #1		36 Hours	Completed / 93
					0800, Aug. 25	
Jan. 23-24	Franklin Lakes NJ	Exercise #3	Exercise #2	Proof of	32 Hours	Completed / 93
	Warminster, PA			Concept	0800, Jan. 23	Completed / 93
				DTS		

- **June 25, 1993** DIS Customer Guide will be mailed out to Agency Disaster Recovery Contacts

Fiscal Year 1994 (July 1993 - June 1994)

Exercise Schedule:

DATE	LOCATION	S/37-VM	UNISYS	TSD	LENGTH OF	STATUS
					EXERCISE	&
					AND START	FY' OF
					TIME (Easterr	EXERCISE
					Standard Time)	
Oct. 16-17 1993	Sterling Forest, NY	Exercise #4	Exercise #3		30 Hours	Completed/94
	Warminister PA.				0200 Oct 16	SAT-SUN
April 9-10 1994	Sterling Forest, NY	Exercise #5	Exercise #4	Exercise #1	48 Hours	Completed/94
	Warminister PA.				0001 Apr. 9	SAT-SUN

- **July 21, 1993 - October 13, 1993** Start weekly planning meetings for the October 16-17, 1993 Disaster Recovery exercise for the IBM and Unisys platforms. These meetings will include setting objectives, identifying staff to be involved, coordinate between affected areas, identify network requirements, identify customer involvement.

- **July 19, 1993** - 10:00-11:30 - Adams Bldg., 1310 Jefferson Street - 2nd Floor Large Conference room - Meet with Agency Disaster Recovery Coordinators and discuss issues regarding the Customer Guide. Call Ken Boling, at 902-3036 to reserve seating.

- **July 20, 1993** - 10:00-11:30 - Adams Bldg., 1310 Jefferson Street - 2nd Floor Large Conference room - Meet with Agency Disaster Recovery Coordinators and discuss issues regarding the Customer Guide. Call Ken Boling, at 902-3036 to reserve seating.

- **July 22, 1993** - 1:00-2:30 - Adams Bldg., 1310 Jefferson Street - 2nd Floor Large Conference room - Meet with Agency Disaster Recovery Coordinators and discuss issues regarding the Customer Guide. Call Ken Boling, at 902-3036 to reserve seating.

- **July 23, 1993** - 10:00-11:30 - Adams Bldg., 1310 Jefferson Street - 2nd Floor Large Conference room - Meet with Agency Disaster Recovery Coordinators and discuss issues regarding the Customer Guide. Call Ken Boling, at 902-3036 to reserve seating.

- **August 5, 1993** - 1:30-3:30 - Adams Bldg, 1310 Jefferson Street - 2nd Floor Large Conference room - Meet with Agency Disaster Recovery Coordinators and other agency staff to discuss agency print concerns, comments, questions, DIS print plans, print priorities. Call Ken Boling, at 902-3036 to reserve seating.

- **August 6, 1993** - 1:30-3:30 - Adams Bldg, 1310 Jefferson Street - 2nd Floor Large Conference room - Meet with Agency Disaster Recovery Coordinators and other agency staff to discuss agency print concerns, comments, questions, DIS print plans, print priorities. Call Ken Boling, at 902-3036 to reserve seating.

- **January 12, 1994 - April 6, 1994** - Start weekly planning meetings for the April 9-10, 1994 Disaster Recovery exercise for the IBM and Unisys platforms. These meetings will include setting objectives, identifying staff to be involved, coordinate between affected areas, identify network requirements, identify customer involvement.

- **During 3rd Quarter of FY'94 (Jan,Feb,Mar. 1994)** - DIS will be scheduling customer sessions to discuss IBM and Unisys Disaster Recovery data backup process. DIS (IBM) will be testing a proposed backup method in the October, 1993 Disaster Recovery exercise. This process will be verified for accuracy before it is presented to our customers. This process is being developed so that the data backup tasks can be turned over to the our IBM/MVS customers. This series of meeting will be followed up by training sessions, which will be scheduled at a later time. All Disaster Recovery Coordinators listed in this document will be sent a notice of the meeting.

- **During 3rd Quarter of FY'94 (Jan,Feb,Mar. 1994)** - DIS will be scheduling customer sessions to discuss IBM and Unisys Disaster Recovery process for Applications, such as ADABAS,Cics, Mapper. DIS will explain the connectivity, availability and other points of interest. All Disaster Recovery Coordinators listed in this document will be sent a notice of the sessions.

- **During 3rd Quarter of FY'94 (Jan,Feb,Mar. 1994)** - TSD will be conducting an exercise to perform a "Proof of Concept" for the Lacey alternate site. This will be a connectivity exercise and will not involve either the IBM or Unisys platforms. The IBM and Unisys sections of TSD are currently working with some of our shared and dedicated Network customers to assist them in relocating some of their lines from OB2 to the new Lacey Network Center.

Fiscal Year 1995 (July 1994 - June 1995)

Exercise Schedule:

DATE	LOCATION	S/37-VM	UNISYS	TSD	LENGTH OF EXERCISE AND START TIME (Eastern Standard Time)	STATUS & FY' OF EXERCISE
Oct. 22-23 1994	Warminster PA.		Exercise #5	Exercise #2	36 Hours Start 0001 10/22/94 End 12 Noon 10/23/94	Completed/95 SAT-SUN
Oct. 21-23 1994	Sterling Forest NY	Exercise #6		Exercise #2	48 Hours Start 12 Noon 10/21/94 End 12 Noon 10/23/94	Completed/95 FRI-SUN
May 20-22 1995	Sterling Forest, NY	Exercise #7		No Test	48 Hours Start 0800 5/20/95 End 0800 5/22/95	Completed/95 SAT-MON
May 20-22 1995	Warminster PA.		Exercise #6	No Test	48 Hours Start 0800 5/20/95 End 0800 5/22/95	Completed/95 SAT-MON

- **August 16, 1994 - October 19, 1994** Start weekly planning meetings for the October 21-23, 1994 Disaster Recovery exercise for the IBM and Unisys platforms. These meetings will include setting objectives, identifying staff to be involved, coordinate between affected areas, identify network requirements, identify customer involvement.

- **March 21, 1995 - May 17, 1995** Start weekly planning meetings for the May 20-22 1995 Disaster Recovery exercise for the IBM and Unisys platforms. These meetings will include setting objectives, identifying staff to be involved, coordinate between affected areas, identify network requirements, identify customer involvement.

Fiscal Year 1996 (July 1995 - June 1996)

Exercise Schedule:

DATE	LOCATION	S/390-VM	UNISYS	TSD	LENGTH OF EXERCISE AND START TIME (Eastern Standard Time)	STATUS & FY' OF EXERCISE
Oct. 28-30 1995	Gaithersburg, MD	Exercise #8		Exercise #3	48 Hours Start 0800 10/28/95 End 0800 10/30/95	Completed/96 SAT-MON
Oct. 28-30 1995	Warminster PA.		Exercise #7	Exercise #3	48 Hours Start 0800 10/28/95 End 0800 10/30/95	Completed/96 SAT-MON
April 27-29, 96	Gaithersburg, MD	Exercise #9		Exercise #4	48 Hours Start 0800 4/27/96 End 0800 4/29/96	Completed/96 SAT-MON
April 27-29, 96	Warminster PA.		Exercise #8	Exercise #4	48 Hours Start 0800 4/27/96 End 0800 4/29/96	Completed/96 SAT-MON

- **February 27 - April 23, 96** Start weekly planning meetings for the April 27-29, 1996 Disaster Recovery exercise for the IBM and Unisys platforms. These meetings will include setting objectives, identifying staff to be involved, coordinate between affected areas, identify network requirements, identify customer involvement.

Fiscal Year 1997 (July 1996 - June 1997)

Exercise Schedule:

DATE	LOCATION	S/390-VM	UNISYS	TSD	LENGTH OF EXERCISE AND START TIME (Eastern Standard Time)	STATUS & FY' OF EXERCISE
Oct. 26-28, 96	Gaithersburg, MD	Exercise #10		Exercise #5	48 Hours Start 0800 10/26/96 End 0800 10/28/96	Pending/97 SAT-MON
Oct. 26-28, 96	Warminster PA.		Exercise #9	Exercise #5	48 Hours Start 0800 10/26/96 End 0800 10/28/96	Pending/97 SAT-MON

IX. Maintenance

Maintenance Cycle

The maintenance of this document will be the responsibility of Ken Boling, Disaster Recovery Manager/Coordinator for DIS. This document will be updated on an as needed basis.

Maintenance Triggers

The Customer Guide will be most easily maintained if changes in the data processing and/or business environment trigger reviews of the document that result in necessary modifications. Some examples of significant changes that may occur at DIS::

- Major modification to an existing application.
- Off-site storage location or procedural changes.
- New software upgrades or installs that could affect our customers
- Changes to the backup process.

Maintenance Record

The purpose of this section is to provide an ongoing record of the changes which have been made to the DIS Customer Guide:

UPDATED	REASON FOR UPDATE	COMMENTS
6/27/94	Numerous changes since original creation date. New Customer Contacts, Additional Exercise dates, Updates phone Directories.	
12/19/94	Quarterly Update	
1/11/96	Numerous updates - Distributed complete new document	
5/28/96	Updates	

Update Confirmation

TO: Ken Boling, Disaster Recovery Manager/Coordinator
Mail stop: 42445

FROM: Customer Guide Holder _____**(Please PRINT Your Name)**

SUBJECT: Confirmation of Updates to the DIS Customer Guide

I have received the updates to the Customer Guide and I have inserted them into the proper sections of my document. **Return address is on back side of form. Fold with address showing. Thank you.**

Signature:_____

Ken Boling
Department of Information Services
MS: 42445

Change Notice

TO: Customer Guide Holders

FROM: Ken Boling, Disaster Recovery Manager/Coordinator

SUBJECT: Updates to the DIS Customer Guide

Attached to this notice are the updates to the DIS Customer Guide. These updates are a result of updated changes. Please incorporate these pages in your manual.

Chapter		Remove Pages	Replacement Pages
	Table of Contents		
I	Introduction		
II	Program History		
III	Program Organization		
IV	Data Backup and Restoration		
V	Output Production Services		
VI	Customer Interface		
VII	Telephone Directory		
VIII	Calendar of Events		
IX	Maintenance		
X	Appendices		

Customer Guide Holders

Name	Phone	MS	Agency
DR Customer Contacts			
Fanette Stewart	360-786-7012	40938	011
Richard Fisher	360-786-7560	40482	012
Steve Lynch	360-786-7060	40938	012
Bob Fitchitt	360-753-5911	40934	020
Curtis Gilbertson	360-753-5911	40934	020
Nate Naismith	360-786-7725	40949	038
Larry Watilo	360-786-7002	40949	038
Patty Frost	360-753-3365	41170	055
Brian Backus	360-753-3365	41170	055
Lori Jones	360-753-4378	43113	075
Jim Anderson	360-753-4573	43113	075
Allen Schmidt	360-664-3373	43125	075
Jim Squire	360-956-2116	43165	077
Jim Columbo	360-956-2027	43165	077
Karen Copeland	360-753-1111	40908	082
Malissa Warheit	360-753-1980	40908	082
Ellen Myers	360-586-8256	40234	085
Rand Daley	360-753-2524	40234	085
James Frost	360-586-2879	40207	090
Patrick Bohlig	360-586-2878	40207	090
Roger Brittingham	360-753-3549	40042	095
Susan Smith	360-586-8504	40031	095
Jim Albert	360-664-0159	40119	100
Dave Finnick	360-664-4317	40119	100
Steve Armstrong	360-586-1398	48300	103
Jackie Jones-Hook	360-586-4505	48300	103
Lori Jones	360-753-4378	43113	105
Mike Contris	360-664-3378	43113	105
Jim Anderson	360-753-4573	43113	105
Allen Schmidt	360-664-3373	43125	105

Customer Guide Holders (Continued)

Name	Phone	MS	Agency
DR Customer Contacts			
Marilyn Tucker	360-923-2851	42710	107
Hieu Ngyen	360-923-2840	42545	107
Gary Maciejewski	360-459-6656	47580	111
Aloha Brown	360-459-6627	47580	111
Mike Bieker	360-586-1090	43045	116
Tom Brewer	360-753-1947	43000	116
Gerald Klein	360-438-7654	42400	117
Jim Gunn	360-753-2530	48380	124
Sharon Megiveron	360-586-4584	48380	124
Tom Edwards	360-664-8297	40916	126
Jim Lee	360-664-8295	40916	126
Mike Cole	360-753-6820	47100	130
Mike Hickox	360-753-6820	47100	130
Carl Schwarmann	360-586-6986	47461	140
Carolyn Hoyt	360-664-0321	47461	140
Ray LeVee	360-586-3504	41014	150
Don Pohlman	360-586-2764	41000	150
Bill Storms	360-438-7657	40257	160
Hanno Oldenburg	360-586-1006	40257	160
Dan Lipp	360-586-6346	42401	190
Larry Ramsey	360-586-6346	42401	190
Jim Plonski	360-753-6345	43102	195
Curt Volland	360-753-9113	43102	195
Bob Klein	360-753-3056	47250	215
Mike Kretzler	360-753-3055	47250	215

Customer Guide Holders (Continued)

Name	Phone	MS	Agency
DR Customer Contacts			
Larry Wassman	360-586-3561	42622	225
Dan Parsons	360-586-7562	42622	225
Lisa Micheau	360-902-4251	44821	235
Bob Marlatt	360-753-6926	49020	240
Mike Roberts	360-586-4541	49020	240
Len Devenere	360-664-4943	48001	240
Ken Raupp	360-902-7615	45889	300
Cheryl Chorba	360-902-7617	45889	300
Bill Allen	360-902-7709	45895	300
Tom Martin	360-705-6110	47904	303
Tom Harmon	360-705-6341	47816	303
Andy Jackson	360-586-8394	41150	305
Wayne Wilkes	360-586-8539	41110	310
Charly Ryman	360-753-0140	41109	310
Patti March	360-586-8539	41110	310
Fay Bronson	360-586-1250	40933	315
Tom Jons	360-753-7890	43430	343
Tom Bohon	360-753-7891	43430	343
Bob Patterson	360-664-0368	47200	350
Ed Strozyk	360-753-1701	47200	350
Mike Scroggins	360-586-8771	42495	352
Liz Baker	360-753-3670	42495	352
David Johnson	509-335-3584	WSU	365
Jim Haugen	509-335-8643	WSU	365
Wayne Praeder	509-359-6915	EWU	370
Stephen Davis	509-359-6685	EWU	370
James Haskett	509-963-2921	CWU	375
Terilee Germain	509-963-2946	CWU	375

Customer Guide Holders (Continued)

Name	Phone	MS	Agency
DR Customer Contacts			
James Johnson	360-866-6000 - x6238	TA-00	376
Dale Baird	360-866-6000- x6237	TA-00	376
Jayne Vaughn	360-650-2978	WWU	380
Richard Porter	360-650-3502	WWU	380
James McClue	360-705-7696	47427	405
Dennis DeFries	360-705-7707	47427	405
Judy Mattingly	360-407-6911	47600	461
Sunny Cotey	360-407-6586	47600	461
Art Brown	360-753-2525	42650	465
Mike Giovanni	360-586-7007	42650	465
Thelma Smith	360-902-3010	40917	467
Debra Wilhelmi	360-902-3005	40917	467
Phil Coates	360-902-2300	43138	477
Debbie Howell	360-902-2334	43138	477
Mary Ellen Bradley	360-902-2303	43138	477
Larry Sugarbaker	360-902-1546	47020	490
Norm Gunther	360-902-1514	47022	490
Phillip Maddalosso	360-902-2007	42565	495
James Martinez	360-902-2004	42560	495
Diane Vasarkovy	360-438-4780	46000	540
Dennis Laine	360-438-3225	46000	540
Thomas Bynum	360-438-4867	46000	540
Carol Lund	360-438-4725	46000	540

Customer Guide Holders (Continued)

Name	Phone	MS	Agency
DR Customer Contacts			
Gary Sigmen	360-566-5007	TCC	678
Wes Morgan	206-803-9737	CTC	699
John Lowdon	206-803-9729	CTC	699
Dennis Bailey	509-372-5395	WPPSS	954
Karen Hughes	509-372-5276	WPPSS	954
Special Interest Group:			
Non DR Customer Contact			
Ray Krontz	360-357-2088	40922	047
Mark Johnson	360-753-3365	41170	055
Debbie Wells	360-753-6565	40021	095
Sharon Novak	360-586-4971	43113	105
Wayne Engle	360-438-3147	43125	105
Ed Ford	360-459-6610	47580	111
Karl Seitz	360-586-6212	43045	116
Jim Stanton	360-586-5777	48380	124
Phil Tenkhoff	360-754-4780	44710	235
Ken Mark	360-586-4541	48001	240
Karen Engvall	360-902-7710	45895	300
Gene Robbins	360-753-1009	45888	300
Fran Muskopf	360-706-6106	47904	303
Tom Martin	360-705-6110	47904	303
Rose Bossio	360-705-6106	47904	303
Donald Smith	360-664-0648	41109	310
Paul Braget	360-753-5424	42460	385

Customer Guide Holders (Continued)

Name	Phone	MS	Agency
Miles Neale	360-459-6051	47600	461
Jim Griffith	360-493-9296	47600	461
Mary Smith	360-902-1505	47020	490
Brad Chandler	360-438-4733	46000	540
Roger Stefan	360-438-4734	46000	540
Others:			
Mike McVicker		42452	155
Mike Curtright		42449	155
John Devereaux		42449	155
Steve Kolodney		42440	155
Clare Donahue		42440	155
Sarah Magnuson	360-587-3497	IBM	IBM
Bob Elias		42442	155

X. Appendices